TRENDS IN RESEARCH: THE ANALYTIC NUMBER THEORY

HANS RADEMACHER

Ladies and Gentlemen: I wish to express my gratitude for the invitation to address this meeting and to thank you for granting me this opportunity to contribute a little part to the celebration of the anniversary of our host, this renowned institution of higher learning, the University of Chicago. The research work emanating from here has in its mathematical branch strongly emphasized analysis as well as number theory. The name "analytic number theory," indicating a union of these two fields of mathematical endeavor, is about as old as this celebrating Institution. In 1894 a book was published under the title *Die Analytische Zahlentheorie*, by Paul Bachmann. The name "analytic number theory" itself was a program. It said more than "diverse applications of infinitesimal calculus to number theory" as Dirichlet, the real founder of our discipline, had modestly called one of his great memoirs (1839). The name "analytic number theory," implies, as I take it, a thorough fusion of analysis and arithmetic, in which as we shall see, analysis is not necessarily subordinate to arithmetic. Incidentally, "analysis" stands here always for function theory, especially the theory of analytic functions.

What has the theory of functions to do with the theory of integers? Let me, to gain a starting point, begin with a few examples of well established results of analytic number theory:

1. If $\pi(x)$ denotes as usual the number of prime numbers less than or equal to x, then

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1 \tag{1}$$

as first proved by Hadamard and de la Vallée Poussin in the nineties of the last century.

2. The number of representations of a positive integer n as a sum of four squares is

$$r_4(n) = 8\left(\sum_{d|n} d - \sum_{4|d'|n} d'\right) \tag{2}$$

as Jacobi found as a corollary of his theory of elliptic functions.

An address delivered before the meeting of the Society in Chicago, Ill., on September 5, 1941, by invitation of the Program Committee; received by the editors January 6, 1942.

3. The number $h(D)$ of classes of positive primitive binary quadratic forms of determinant $D \equiv 7 \pmod 8$ is given by Dirichlet's formula

$$h(D) = \sum_a \left(\frac{a}{D}\right) \tag{3}$$

where $(a, D) = 1$, and a runs through all positive integers less than $(1/2)D$.

Now, the first of these examples makes it quite obvious that analysis has to be applied, since the result does not only contain the continuous function $x/\log x$, but moreover involves the notion of limit, so that the two fundamental concepts of infinitesimal analysis are represented in (1).

This is not so in the two other examples. All expressions appearing in the equations (2) and (3) have an arithmetical meaning and are defined in elementary number theory without any reference to analysis. Nevertheless both results appear as the goal of analytic proofs in one of which appear ϑ-functions and in the other Dirichlet series. Both theorems can therefore be claimed by analytic number theory. However, there remains a big difference in these two cases: whereas the result (2) can also be proved by purely arithmetical methods, the equation (3) has defied all attempts of an elementary arithmetical proof.

This observation raises the question, which I will state in all its logical vagueness: what is the connecting link between arithmetic and analysis, or by what means can analysis take hold of arithmetical facts? In the steady flow of real numbers, called the continuum, which is the substratum of function theory, the integers are in no way distinguished from any other real numbers. The function e^z at first glance has no "affinity" to integers. We notice, however, the relation

$$e^{2\pi i z} = e^{2\pi i(z+n)}$$

for any integer n and all complex values z. The function has *the period* n where n can be any integer. The fundamental fact is that the periods of an analytic, or for that matter, a continuous function form a discrete module or lattice. Or, speaking a little more generally: the ideas connected with period, invariance, and substitution group are basic for the application of analysis to number theory, and, as we can remark already here, also for the inverse process. Let me give another example, which is a little more involved. For the modular invariant $J(\tau)$ we know that

$$J(\tau) = J(\tau') \tag{4a}$$

implies and is implied by

$$\tau' = \frac{a\tau + b}{c\tau + d}, \qquad ad - bc = 1, \tag{4b}$$

a, b, c, d being integers. The function $J(\tau)$ appears thus as an embodiment of the discrete group of modular substitutions. This fact must have implications in both directions. Indeed, the group of modular transformations defines the classes of binary quadratic forms, and so we are led to the theory of singular moduli, the theory of complex multiplication, and finally to the Kronecker-Fueter theorem that any Abelian field over an imaginary quadratic field can be generated by the values of certain modular forms which they attain for special imaginary quadratic irrationalities. On the other side, equations (4a) and (4b) lead function-theoretically to the expansion (Petersson [**33**, **37**])

$$12^3 J(\tau) = e^{-2\pi i\tau} + 744 + \sum_{n=1}^{\infty} c_n e^{2\pi i n\tau} \tag{5a}$$

with

$$c_n = \frac{2\pi}{n^{1/2}} \sum_{k=1}^{\infty} \frac{1}{k} I_1\left(\frac{4\pi n^{1/2}}{k}\right) \sum_{h \bmod k,\,(h,k)=1} e^{-(2\pi i/k)(nh+h')},\ hh' \equiv -1 (k), \tag{5b}$$

where $I_1(z) = -iJ_1(ix)$, the Bessel function of the first order.

You will always find such a group-invariance or periodicity, sometimes conspicuous, sometimes concealed, as underlying the applications of analysis to number theory. Fourier series, Fourier integrals, and Poisson sums are, therefore, natural and frequently used tools. But also the configuration of a point lattice can be taken as to express periodicity (especially in Minkowski's work in the "geometry of numbers"), and even a power series is here often better understood as a series in $e^{2\pi iz}$, that is, a Fourier series with its obvious periodicity.

These analytic tools, developed in the 19th century, indicate sufficiently that our discipline must be a rather young one, so very much younger than elementary number theory, in whose history we meet the names of Euclid, Diophantos, Fermat. Indeed Lejeune Dirichlet can be regarded as the founder of our branch of research. Before him Euler, Gauss, and especially Jacobi, had found methods and results belonging to this field. After Dirichlet it was Riemann who with his epoch making memoir *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse* (1859) made the deepest mark in its history. In this brief survey I have also to mention the names of Hermite, Kronecker,

Hadamard, de la Vallée Poussin, and Minkowski, who all contributed works of lasting value.

The *present* standing of analytic number theory and its recognition as a fruitful branch of our science is, I think, entirely due to three mathematicians of this century: Landau, Hardy, and Littlewood. To Hardy and Littlewood we owe important progress in the theory of prime numbers and in our knowledge of the distribution of the complex zeros of the ζ-function. Their greatest contribution, which they share with Ramanujan, lies, however, in the development of a fundamentally new method in additive number theory, a method which yielded their celebrated theorems concerning partitions, and about additive representations of numbers as sums of powers (Waring's problem) and as sums of primes (Goldbach's problem).

Landau has exerted a wide influence through his untiring mathematical enthusiasm and through his forceful advocacy of utter precision. The substance of his work has proved to be less permanent; his results were soon surpassed by deeper and more comprehensive ones, and his papers have very often been only second redactions of discoveries of others. How much we owe him nevertheless becomes evident if we compare a publication on analytic number theory of the the 1890's (for example, the above mentioned book of Bachmann, but also such substantial papers like those of Hadamard and de la Vallée Poussin not excepted) with a contemporaneous paper. Landau developed the technique of analytic number theory and prepared the tools; he found certain theorems about power series, Dirichlet series, Fourier integrals, which now are generally used as lemmas; and he made us familiar with the usefulness of a number of devices and lemmas discovered by others, as for example, Abel's partial summation, Mellin's formula, and Carathéodory's lemma. Landau's handbook on prime numbers will remain a classical treatise. Not a small merit of it is that it shaped our notation: It brought the symbol "O" into general use (it had been invented by Pringsheim), and Landau introduced there the symbol "o" (a constant source of quarrel between him and Pringsheim, which the German mathematicians used to watch with amusement). Both these symbols, now so well known and generally adopted, are particularly fit to express asymptotic relations which so frequently occur in analytic number theory.

Landau is no longer with us; Hardy and Littlewood about 10 years ago turned to other fields of investigation. Hence I understand it as my main task today to give a survey of developments in analytic number theory which took place after these three outstanding authors and independent of them.

This development has proceeded chiefly in two directions. One of them can roughly be characterized by words like "asymptotic formula" and "error term;" inequalities play an important part in the technique to "estimate" the error. I think here mainly of problems like the prime number theorem, lattice points in the circle, asymptotic expressions for the number of representations of a number as a sum of one or the other sort, investigations in which Hardy, Littlewood, and Landau have distinguished themselves, so that this pursuit of research can be understood as a direct continuation of their work. Investigations of this sort have attracted general attention, so much so, indeed, that the impression may have prevailed that analytic number theory deals foremost with asymptotic expressions for arithmetical functions. This view, however, overlooks another side of analytic number theory, which I may indicate by the words "identities," "group-theoretical arguments," "structural considerations." This line of research is not yet so widely known; it may very well be that methods of its type will lead to the "deeper" results, will reveal the sources of some of the results of the first direction of approach. Remarks like those which I made about applicability of analysis to arithmetic are especially pertinent here. The names Artin, Hecke, Mordell and Siegel would have to be mentioned in this connection.

The first type of analytic number theory is at present carried on in the Russian school with Vinogradoff as the leading name. Vinogradoff has become widely known for his great contributions to Waring's problem and Goldbach's problem. In this work he depends entirely on Hardy's and Littlewood's precedency; he introduced essentially two improvements of their method. One is of minor importance and merely an affair of convenience. He observed that for the additive representation of the number n you obviously do not need summands surpassing n. This means that the power series which have been used by Hardy and Littlewood (and whose use in additive number theory really dates back to Euler) can be replaced by polynomials. This has certain advantages since it discards the difficulty of the natural boundary which the unit circle represents for those power series. Vinogradoff's second and decisive advance lies in his ingenious estimate of certain sums of roots of unity, as I shall now try to explain.

I begin with Waring's problem, in whose treatment Vinogradoff reaped his first success. For the discussion of

$$f(x) = \sum_{n=0}^{\infty} x^{n^k} \tag{6}$$

in the neighborhood of a root of unity $\xi = e^{2\pi i(h/q)}$ Hardy and Little-

wood need expressions for the sums

$$S_q(M) = \sum_{n=0}^{M} e^{2\pi i(h/q)n^k} \tag{6a}$$

with the emphasis upon their dependence on q and M (for fixed given $k \geqq 3$; $k=2$ is in a different class since $f(x)$ is then essentially a ϑ function and $S_q(M)$ essentially a Gaussian sum, both of which are well known from other connections). Now for an M which is large compared with q an expression with a useful error term is easily found by partial summation. The error term, however, becomes unmanageable for q comparatively large. This case, which appears on the so-called "minor arcs" proved first to be a serious obstacle to Hardy's and Littlewood's efforts. It is known that this difficulty delayed their final success for two years at a time when the required device had already been found and published by H. Weyl [58] but due to the interruption of communications during the first World War had not yet come to Hardy's and Littlewood's notice.

Now Vinogradoff recognized that a certain k-fold iteration in Weyl's method could be dispensed with and replaced by one single step. Since that iteration was the source of a factor 2^k in the estimate for $G(k)$, the smallest number of kth powers sufficing to express every sufficiently large number additively, this change meant an extraordinary diminution of the estimated order of $G(k)$, a diminution as a matter of fact which was so considerable that it enabled Dickson to establish in many cases the true value $g(k)$ of kth powers which suffice to represent additively *all* positive integers, simply by bridging the finite gap not covered by $G(k)$ through a number of elementary computational steps [6, 7].

Vinogradoff's lemma, which replaces Weyl's lemma, can be enunciated as follows (in the form which was given to it by Heilbronn [21]):

Let x run through X integers of an interval of length L, y through Y integers on an interval of length M, then

$$\left|\sum_{x,y} e^{2\pi i(xy/q)}\right|^2 \leqq \frac{XYML}{q}\left(1+\frac{q}{M}\right)\left(1+\frac{q\log q}{L}\right). \tag{7}$$

This lemma is not immediately applicable to (6a) and to (6). Vinogradoff employs the astonishing device of dropping certain Waring representations of the given number n, by selecting kth powers of a certain factorization. This diminishes the chance of a Waring representation. Nevertheless he finds that the number of representations is different from null for $s \geqq 6k\log k+(4+\log 216)k$ summands and sufficiently large n [50].

Vinogradoff's most startling achievement was his proof in 1937 that every large odd number is the sum of three primes [52, 53], a result previously obtained by Hardy and Littlewood only under a generalized Riemann hypothesis. Vinogradoff's result is so far the closest approach to Goldbach's conjecture ever reached. The difficulties are here much greater than for the Waring problem, the distinction between major and minor arcs much subtler. The major arcs require for their treatment the classical theory of the distribution of primes founded on the ζ-function and the Dirichlet L-functions. In Vinogradoff's paper, moreover, a deep theorem of Siegel about the class-number of quadratic fields [46] was used, which can be expressed in the statement

$$|L(1, \chi)| > \frac{C}{k^{\epsilon}}$$

where χ is a real character modulo k, a theorem which widens Heilbronn's result [22] that the number of imaginary quadratic fields of class-number one is finite. Walfisz thereafter showed that Siegel's theorem can be dispensed with, at the cost of some loss of precision in the error term [54].

The sum to be appraised in Goldbach's problem is

$$T_q(M) = \sum_{p \leq M} e^{2\pi i (h/q) p},$$

again in particular for the minor arcs, that is, for comparatively high denominator q. Now this sum does not fit into the scheme of Vinogradoff's lemma (7) since p alone and not a product appears in the exponent. Vinogradoff resorts here to the sieve of Eratosthenes [53] which had been so successfully used by Viggo Brun [3]. The argument runs like this:

$$T_q(M) = \sum_{r=2}^{M} e^{2\pi i (h/q) r} - \sum_{p_1 \leq M^{1/2}} \sum_{2 \leq m \leq M/p_1} e^{2\pi i (h/q) m p_1} + \sum_{p_2 < p_1 \leq M^{1/2}} \sum_{1 \leq m \leq M/p_1 p_2} e^{2\pi i (h/q) m p_1 p_2} + \cdots .$$

The first sum is a trivial geometric sum, and in the following sums we do find the desired products in the exponents. This opens the way to an application of (7). Still, the completion is not quite simple but is handled by Vinogradoff with superb technique. I have already quoted his final result regarding Goldbach's problem.

Before I drop this strand of my narration I wish to mention Tchudakoff's application of Vinogradoff's methods to the estimation of Riemann's ζ-function on $\Re(s) = 1$ [49]. Tchudakoff uses Vinogra-

doff's estimates [51] in the same way as Littlewood and Landau had used Weyl's method for the improvement of the error term in the prime number theorem to $O(x \exp(-a(\log x \log\log x)^{1/2}))$. Tchudakoff obtains the prime number theorem in the form

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O(xe^{-a(\log x)^{\alpha}})$$

with a certain $\alpha > 1/2$. Until then the remainder term had for three decades shown the value $\alpha = 1/2$. Of course, any $\alpha < 1$ is still far off from the Riemann hypothesis which is equivalent to $\alpha = 1, a = (1/2) - \epsilon$.

Appraisals of sums of roots of unity have recently played an important role in several parts of analytic number theory. Mordell [31], Davenport [4], and Hasse [5, 14] discussed sums of the form

$$S_q = \sum_{n \bmod q} e^{(2\pi i/q) f(n)}$$

where $f(n)$ is a polynomial in n with integral coefficients. The aim is to give an estimate of S_q with respect to q. The problem is a generalization of the order of magnitude of Gaussian sums, that is, $f(n)$ of the second degree, in which case we have

$$S_q = O(q^{1/2}).$$

It is of interest that the exponent $1/2$ which appears here in a number of cases has something to do with the abscissa $\Re(s) = 1/2$ in the Riemann hypothesis, not for the ordinary ζ-function, it is true, but for the ζ-function belonging to a field of algebraic functions over a finite field of characteristic p; these ζ-functions were introduced by E. Artin [1] in 1924 and later in a more general form defined by F. K. Schmidt [44]. The non-trivial zeros ρ of such a ζ-function turn out to be periodic and given by

$$\beta = p^{\rho}$$

where β are the roots of certain polynomials; clearly $|\beta| = p^{1/2}$ means

$$(*) \qquad \Re(\rho) = 1/2,$$

and the absolute value of β depends on the number of solutions of certain congruences modulo p, or, which is equivalent to this, on the value of certain exponential sums. Relation (*) has been proved for the Artin ζ-functions of the field of elliptic functions by Hasse [12, 13], who also outlined a program for further research. Modern algebraic concepts are fundamental in this work. Quite recently, in this year, André Weil [56, 57] published two sketches of proofs for the

Riemann hypothesis in all algebraic function fields over a finite field. We are looking forward to a complete account of his proof. Here still a wide field is open to research, a field attractive at the same time by its large generality and its richness of specific details.

A particularly interesting case of sums of roots of unity are the so-called Kloosterman sums

$$S_q(u, v) = \sum_{h \bmod q,\,(h,q)=1} e^{(2\pi i/q)(uh+vh')}$$

with $hh' \equiv 1 \pmod{q}$. Since these sums are multiplicative with respect to q, they can be broken down to those with prime-number powers q. For $q = p^\alpha$, $\alpha \geqq 2$, the order $O(q^{1/2})$ has been established by Salié [43], and moreover an explicit formula involving Legendre symbols and trigonometric functions has been found. Surprisingly, however, the case of a prime number $q = p$ offers difficulties which so far have only permitted us to prove

$$S_p(u, v) = O(p^{2/3}).$$

Weil's above-mentioned results should establish here also $O(p^{(1/2)+\epsilon})$.

The Kloosterman sums appear in the theory of partitions and in the study of the coefficients of modular functions. Recent work connected with these problems can also be understood as an extension of the Hardy-Littlewood-Ramanujan work. Whereas Hardy and Ramanujan obtained only an asymptotic expression for the number $p(n)$ of partions of n, a refinement and at the same time a simplification of their method led to the equation [35, 36]

$$p(n) = \frac{1}{\pi 2^{1/2}} \sum_{q=1}^{\infty} A_q(n) \frac{d}{dn} \left\{ \frac{\sin h \dfrac{K}{q} \left(n - \dfrac{1}{24}\right)^{1/2}}{\left(n - \dfrac{1}{24}\right)^{1/2}} \right\},$$

$$A_q(n) = \sum_{h \bmod q,\,(h,q)=1} \omega_{h,q} e^{-2\pi(hn/q)}, \quad K = \pi(2/3)^{1/2},$$

where $\omega_{h,q}$ are certain roots of unity taken from the theory of transformation of the modular form $\eta(\tau)$, which have attracted the attention of quite a number of mathematicians since Hermite. The series in the equation just mentioned is absolutely convergent. It has been used successfully by D. H. Lehmer for the numerical computation of $p(n)$ for high values of n [26, 27]. Analogous results for other problems of partitions with certain congruence conditions imposed on the summands have been obtained by Zuckerman [59], Niven [32], Hua [23], Miss Haberzetle [9], and Lehner [28].

These investigations form a natural bridge between the two different ways of investigation I mentioned before. Technically they require estimates of error terms, but also some group-theoretical arguments. And they lead to identities, which in turn invite group-theoretical treatment and thus point in the second direction in our field.

Identities can be used as sources of other identities. In this way the famous Ramanujan identities, of which I quote here only

$$(**) \qquad \sum p(5l+4)x^l = 5\Big[\prod (1-x^{5q\,m})^5 \Big/ \prod (1-x^m)^6\Big],$$

can be proved by direct comparison of coefficients which are known in forms of series through the just mentioned methods. But the true source of the Ramanujan identities lies in the theory of transformation of modular forms, as it is seen at once if we rewrite the identity (**)

$$\sum_{\lambda=0}^{4} \frac{1}{\eta\left(\dfrac{\tau+24\lambda}{5}\right)} = 5^2 \frac{\eta(5\tau)^5}{\eta(\tau)^6}$$

[30, 39].

The formula (5) is an identity, which can also be derived by the Hardy-Littlewood-Ramanujan method. Here the problem arises to understand the invariance

$$J\left(\frac{a\tau+b}{c\tau+d}\right) = J(\tau)$$

as an outcome of the Fourier series on the right-hand member [38].

Hardy himself has contributed a remarkable paper to similar investigations [10], showing that for example,

$$\vartheta_3^8(0,\tau) = 1 + \frac{\pi^4}{3!}\sum_{n=1}^{\infty} n^3 S_8(n) e^{2\pi i n\tau},$$

(8a)

$$S_8(n) = \sum_{q=1}^{\infty} \frac{1}{q^8} \sum_{h \bmod q,\,(h,q)=1} \left(\sum_{j=1}^{q} e^{2\pi i(hj^2/q)}\right)^8 e^{-2\pi i(hn/q)}.$$

Here $S_8(n)$ is the "singular series" of the problem of expressing a number as a sum of 8 squares. The proof of (8a) has to establish the fact that the Fourier series on the right of (8a) is a modular form of dimension -4.

The "singular series," first introduced into analytic number theory by Hardy and Littlewood, form objects of great mathematical interest of their own. They appear in problems of representation of integers in an additive way, for example, as $n = x_1^k + \cdots + x_r^k$. For the

number of representations the Hardy-Littlewood method yields an asymptotic result of the form

$$N_r(n) \sim f_r(n) \cdot \mathfrak{S}_r(n),$$

where $f_r(n)$ is a continuous function of n, which can be interpreted as a density with respect to the r-dimensional point lattice. The other factor is the singular series $\mathfrak{S}_r(n)$, an arithmetical function of n. A remarkable feature of all singular series is that they are factorable according to prime numbers:

$$\mathfrak{S}_r(n) = \prod_p A_p^{(r)}(n). \tag{8b}$$

This fact finds its explanation in the meaning of $A_p^{(r)}(n)$. Whereas for the problem

$$n = x_1^k + \cdots + x_r^k$$

the function $f_r(n)$ means the derivative

$$f_r(n) = \frac{d}{dn} V_r(n)$$

of the volume

$$V_r(n) = \int \cdots \int_{x_1^k + \cdots + x_r^k \leqq n; 0 \leqq x_j} dx_1 \cdots dx_r$$

or, in other words, a measure of the area of the surface

$$n = x_1^k + \cdots + x_r^k, \qquad 0 \leqq x_j; j = 1, \cdots, r,$$

the $A_p^{(r)}(n)$ give the density of solutions of the congruence

$$n \equiv x_1^k + \cdots + x_r^k \pmod{p^l} \tag{9}$$

with respect to high powers of p as modulus, or explicitly:

$$A_p^{(r)}(n) = \lim_{l \to \infty} \frac{b^{(r)}(n; p^l)}{g^{(r)}(p^l)}$$

where $b^{(r)}(n; p^l)$ is the number of different solutions of (9) and $g^{(r)}(p^l)$ is the average of the number of solutions of (9), distributed over p^l different n's,

$$g^{(r)}(p^l) = \frac{p^{lr}}{p^l} = p^{l(r-1)}.$$

The multiplicativity of the $A_q^{(r)}(n)$ now becomes understandable, and

the product (8*b*) means that $\mathfrak{S}_r(n)$ is the density of solutions of the congruence for, let us say, $m!$ as modulus with $m \to \infty$.

Recently Siegel has emphasized this interpretation and used it with great success in his analytic theory of quadratic forms [47]. In that connection the singular series had appeared before, in the works of Smith and Minkowski, as measure of genera of quadratic forms. Through this connection it becomes clear why the Hardy-Littlewood method leads to an exact formula for the number of representations of n as a sum of r squares for $5 \leqq r \leqq 8$, whereas for higher r it yields only an asymptotic result.

This interpretation of the singular series is possible in all those problems of additive number theory which preassign the number of summands or variables, as in Goldbach's problem, Waring's problem, or mixed problems, as for example, the problem of representation as a sum of a square and two primes (Estermann [8]), or as a sum of r squares and s cubes. It fails, however, for problems with an undetermined number of variables, as in the case of unrestricted partitions, since there the transition from equation to congruence destroys the boundedness of the number of variables for each n, so that the number of solutions modulo p becomes meaningless. Indeed, the formula for $p(n)$, given above, is of quite a different structure.

Singular series appear as coefficients of Fourier series as in (8a). Siegel's analytic theory of quadratic forms can be regarded as a brilliant example of the study of such series. He shows that his series can be combined of ϑ-functions

$$\vartheta(\tau) = \sum_{m_1, \cdots, m_r} e^{2\pi i \tau Q(m_1, \cdots, m_r)}$$

where Q is a positive quadratic form with integral coefficients; such a combination includes ϑ-functions constructed with quadratic forms Q of all classes of the same genus. It is known that such ϑ-series are modular forms of dimension $-r/2$ and of a certain "level" (Stufe) depending essentially on the discriminant of the quadratic form $Q(m_1, \cdots, m_r)$ [45].

A general study of power series with singular series as coefficients has not yet been undertaken. It would be desirable to know more specific details about these functions than the general properties which can immediately be derived from Kac's, van Kampen's, and Wintner's remark [24, 25] that the singular series give rise to almost periodic arithmetical functions of n and from Bochner's and Bohnenblust's [2] theorems about power series with almost periodic coefficients.

The modular functions have from the beginning of our discipline played an important part in *additive* problems; I need in this respect only point to Euler's formula, fundamental for the whole theory of partitions

$$1 + \sum_{n=1}^{\infty} p(n)x^n = 1/\prod_{1}^{\infty}(1 - x^m)$$

in which the denominator is essentially the modular form

$$\eta(\tau) = e^{\pi i\tau/12}\prod_{1}^{\infty}(1 - e^{2\pi i m\tau}),$$

or to equation (2), obtained by Jacobi from an expression for the 4th power of $\vartheta_3(0, \tau)$. Recently, however, they have also appeared in *multiplicative* number theory through the discovery of a surprising and most fruitful connection between modular functions and prime numbers. This connection is elaborated by Hecke in his beautiful theory, of which he published the first account in 1935 in the Royal Danish Academy [16]. As a matter of fact, a special result of Hecke's theory was anticipated by Ramanujan [41, 11] in a conjecture which was then proved by Mordell in 1917 [29]. This is again an instance of Ramanujan's gift of divination; not only that he foresaw or unveiled hitherto unknown facts, but most of his conjectures lead back to sources of great depth and abundant yield.

The "discriminant" in the theory of elliptic functions

$$\Delta(1, \tau) = g_2^3 - 27g_3^2 = (2\pi)^{12}x((1 - x)(1 - x^2)\cdots)^{24}$$

with $x = e^{2\pi i\tau}$ is a modular form of dimension -12, since for a modular substitution

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we have

$$\Delta\left(1, \frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{12}\Delta(1, \tau).$$

The infinite product can be expanded into a power series

$$x\prod_{1}^{\infty}(1 - x^m)^{24} = \sum_{n=1}^{\infty}\tau(n)x^n.$$

If we now, following Ramanujan, associate with this power series the Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s},$$

it turns out that this series can be written as an infinite product

$$F(s) = \prod_{p} \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}}, \tag{10}$$

extended over all primes p. It is appropriate to call such a product an "Euler product" in view of the formula

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}},$$

first found and utilized by Euler. I shall have to make a remark about this latter product a little later. Not only the Euler product (10), but also a functional equation for $F(s)$: $(2\pi)^{-s}\Gamma(s)F(s) = (2\pi)^{s-12}\Gamma(12-s) \cdot F(12-s)$ reminds us strongly of the ζ-function and allied functions.

The coordination of a modular function on the one side and a Dirichlet series satisfying a functional equation on the other has now been systematized by Hecke [17, 18, 19]. Let us take an entire modular form $F(\tau)$ of dimension $-k$, k a positive even integer,

$$F\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k F(\tau)$$

having the expansion

$$F(\tau) = c_0 + \sum_{n=1}^{\infty} c_n x^n, \qquad x = e^{2\pi i \tau},$$

which is everywhere convergent in the upper τ-half-plane. Then let us put

$$\phi(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s} \quad \text{(without } c_0\text{)}.$$

Then the following statements are valid:

(1) The series for $\phi(s)$ is absolutely convergent in the half-plane $\Re(s) > k$.

(2) $\phi(s)$ is an entire function if $c_0 = 0$; if $c_0 \neq 0$ then $\phi(s)$ has a pole of the first order at $s = k$ with the residue $(-1)^{k/2}c_0(2\pi)^k/\Gamma(k)$ and $(s-k)\phi(s)$ is an entire function.

(3) $\phi(s)$ satisfies a functional equation:

$$(2\pi)^{-s}\Gamma(s)\phi(s) = (-1)^{k/2}(2\pi)^{s-k}\Gamma(k-s)\phi(k-s).$$

(4) $(s-k)\phi(s)$ is of finite order.

Of these statements (1) is implied by $c_n = O(n^{k-1+\epsilon})$, which in turn is a simple consequence of the dimension $-k$. For (2) and (3) we have the pattern of Riemann's classical proof for the continuation and the functional equation of the ζ-function by means of a ϑ-function. In its application here the proof runs like this:

We have from Euler's integral

$$\frac{\Gamma(s)}{(2\pi n)^s} = \int_0^\infty e^{-2\pi n y} y^{s-1} dy$$

and therefore for $\Re(s) > k$

$$(2\pi)^{-s}\Gamma(s)\phi(s) = \int_0^\infty (F(iy) - c_0) y^{s-1} dy$$

with

$$F(iy) - c_0 = \sum_{n=1}^{\infty} c_n e^{-2\pi n y}.$$

Since for the modular substitution

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

we have $F(i/y) = (iy)^k F(iy)$ we can write

$$\begin{aligned}
&(2\pi)^{-s}\Gamma(s)\phi(s) \\
&= \int_1^\infty (F(iy) - c_0) y^{s-1} dy + \int_0^1 ((iy)^{-k} F(i/y) - c_0) y^{s-1} dy \\
&= \int_1^\infty (F(iy) - c_0) y^{s-1} dy + i^{-k} \int_1^\infty F(iw) w^{k-s-1} dw - \frac{c_0}{s} \\
&= \int_1^\infty (F(iy) - c_0) y^{s-1} dy + (-1)^{k/2} \int_1^\infty (F(iw) - c_0) w^{k-s-1} dw \\
&\quad + (-1)^{k/2} c_0 \int_1^\infty w^{k-s-1} dw - \frac{c_0}{s} \\
&= \int_1^\infty (F(iy) - c_0)(y^s + (-1)^{k/2} y^{k-s}) \frac{dy}{y} \\
&\quad - c_0 \left(\frac{1}{s} + (-1)^{k/2} \frac{1}{k-s} \right).
\end{aligned}$$

So far our reasoning required $\Re(s) > k$. Now we have arrived at an expression which remains meaningful for any complex s. We have, therefore, obtained an analytic continuation over the whole s-plane for $\phi(s)$. Moreover, the substitution $s \to k - s$ changes the right-hand member by the factor $(-1)^{k/2}$, which proves (3). At the same time we infer the validity of statement (2).

The argument runs also in reverse, from the Dirichlet series of properties (1) to (4) to a modular form of dimension $-k$. Instead of the Euler integral we have only to apply Mellin's formula.

Up to this point we have not encountered any trace of prime numbers. Hecke came to an Euler product by considering not a single modular form, but the whole set of all entire modular forms of dimension $-k$. They constitute a linear family of finite rank κ; the number κ of linearly independent modular forms in this set is a known function of k. A linear operator T will map the whole set on itself. If the system $F^{(\rho)}(\tau)$, $\rho = 1, 2, \cdots, \kappa$ forms a basis then there exists a matrix $(\lambda_{\rho\sigma})$ such that

$$T(F^{(\rho)}(\tau)) = \sum_{\sigma=1}^{\kappa} \lambda_{\rho\sigma} F^{(\sigma)}(\tau).$$

As linear operator Hecke takes, for any natural number n,

$$T_n(F) = n^{k-1} \sum_{a\,d=n} \sum_{b \bmod d} F\left(\frac{a\tau + b}{d}\right) d^{-k},$$

for which it can be proved, by consideration of the subgroup

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n}$$

and its factor-group in the full modular group, that it furnishes again a modular form of dimension $-k$.

Hence we have

$$T_m(F^{(\rho)}(\tau)) = \sum_{\sigma=1}^{\kappa} \lambda_{\rho\sigma}(m) F^{(\sigma)}(\tau).$$

The application of the operator T_m on the Fourier expansion

$$F^{(\rho)}(\tau) = \sum_{n=0}^{\infty} a^{(\rho)}(n) e^{2\pi i n \tau}$$

yields by comparison of coefficients,

$$\sum_{\sigma=1}^{\kappa} \lambda_{\rho\sigma}(m) a^{(\sigma)}(n) = \sum_{\delta \mid m, \delta \mid n} \delta^{k-1} a^{(\rho)}\left(\frac{mn}{\delta^2}\right), \qquad m \geqq 1,\ n \geqq 1. \tag{11}$$

It is decisive that here the right-hand member shows symmetry in m and n, which therefore must also prevail in the left-hand member:

$$\sum_{\sigma=1}^{\kappa} \lambda_{\rho\sigma}(m)a^{(\sigma)}(n) = \sum_{\sigma=1}^{\kappa} \lambda_{\rho\sigma}(n)a^{(\sigma)}(m).$$

The matrix $(\lambda_{\rho\sigma}(0))$, which appears here for the first time, can be uniquely determined as to fulfill also this relation. Now we obtain

$$T_m(F^{(\rho)}(\tau)) = \sum_{\sigma=1}^{\kappa} \lambda_{\rho\sigma}(m) \sum_{n=0}^{\infty} a^{(\sigma)}(n)e^{2\pi i n\tau}$$

$$= \sum_{\sigma=1}^{\kappa} a^{(\sigma)}(m) \sum_{n=0}^{\infty} \lambda_{\rho\sigma}(n)e^{2\pi i n\tau}.$$

This leads to the introduction of the functions

$$f_{\rho\sigma}(\tau) = \sum_{n=0}^{\infty} \lambda_{\rho\sigma}(n)e^{2\pi i n\tau}$$

which span up the same linear set $\{F^{(1)}(\tau), \cdots, F^{(\kappa)}(\tau)\}$ and of which it is easily seen that they belong to the same set. With $\lambda(n) = (\lambda_{\rho\sigma}(n))$ we have in

$$B(\tau) = \sum_{n=0}^{\infty} \lambda(n)e^{2\pi i n\tau}$$

a matrix of modular forms. In connection with (11) it is found that

$$\lambda(m)\cdot\lambda(n) = \sum_{d|(m,n)} d^{k-1}\lambda\left(\frac{mn}{d^2}\right), \tag{12a}$$

which in particular for $(m, n) = 1$ furnishes

$$\lambda(m)\cdot\lambda(n) = \lambda(mn) \tag{12b}$$

and also shows that the different matrices $\lambda(n)$ are commutative.

Now we go over with Hecke to a set of associated Dirichlet series

$$\Phi(s) = (\phi_{\rho\sigma}(s)) = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s},$$

a matrix which, of course, stands for

$$\phi_{\rho\sigma}(s) = \sum_{n=1}^{\infty} \frac{\lambda_{\rho\sigma}(n)}{n^s}, \qquad \rho, \sigma = 1, \cdots, \kappa.$$

Since each element of this matrix is associated to the modular form

$f_{\rho\sigma}(\tau)$ we infer the validity of statements (1) to (4) for each element and hence the functional equation

$$(2\pi)^{-s}\Gamma(s)\Phi(s) = (-1)^{k/2}(2\pi)^{s-k}\Gamma(k-s)\Phi(k-s)$$

in matrix notation. The relation (12b) makes it evident that we can write

$$\Phi(s) = \prod_p \sum_{l=0}^{\infty} \frac{\lambda(p^l)}{p^{ls}}$$

in which the summation of each infinite series can be effectuated by means of (12a) with the result:

$$\Phi(s) = \prod_p (\lambda(1) - \lambda(p)p^{-s} + \lambda(1)p^{k-1-2s})^{-1},$$

where $\lambda(1)$, according to definition, is the unit matrix of order κ. Here we have the analogue of the Euler product.

If we would start the whole process with a new basis, obtained from the former one by a linear substitution A, we would obtain the transformed matrices

$$\lambda^*(n) = A \cdot \lambda(n) \cdot A^{-1}$$

in our results. Such a transformation can be used to get matrices $\lambda(n)$ of an especially simple type. Since the $\lambda(n)$ are commutative they can simultaneously be transformed into matrices in which all elements beneath the principal diagonal are zeros. Beyond this H. Petersson [34] has shown that the λ's can be brought simultaneously into diagonal form, which means that we can start the process with κ linearly independent "eigen-functions" of all the linear operators

$$T_n(F^{(\rho)}(\tau)) = \lambda^*_{\rho\rho}(n)F^{(\rho)}(\tau), \qquad n = 1, 2, \cdots.$$

Petersson proves this in a very elegant manner by introducing a definition of orthogonality of modular forms based on integrals extended over the fundamental region. The $\lambda^*_{\rho\rho}$ are real algebraic numbers. We have now the Dirichlet series

$$\phi_{\rho\rho}(s) = \sum_{n=1}^{\infty} \frac{\lambda^*_{\rho\rho}(n)}{n^s} \tag{13a}$$

with an ordinary Euler product

$$\phi_{\rho\rho}(s) = \prod_p \frac{1}{1 - \lambda^*_{\rho\rho}(p)p^{-s} + p^{k-1-2s}}, \qquad \rho = 1, \cdots, \kappa, \tag{13b}$$

which is exactly of the form as it appears in Ramanujan's work on $\Delta(1, \tau)$. Summarizing, we can roughly say that the Riemann functional equation of a Dirichlet series already implies the Euler factorization with respect to prime numbers, certainly a result in which analytic and arithmetic elements are inseparably welded together.

Unfortunately, Riemann's original coordination of a modular form and a Dirichlet series, namely,

$$\vartheta(\tau) = \frac{1}{2} + \sum_{n=1}^{\infty} e^{\pi i n^2 \tau}, \qquad \zeta(2s) = \sum_{n=1}^{\infty} \frac{1}{n^{2s}}$$

with the Euler product

$$\prod_{1}^{\infty} (1 - p^{-2s})^{-1}$$

does not fit into the scheme, as already the comparison of this Euler product with (13b) shows; indeed, $\vartheta(\tau)$ has the dimension $-1/2$, and for fractional dimensions the complicated transformation formulae introduce multipliers which interfere with the definition of the operators T_n.

Let us go back for a moment to the functions $\phi_{pp}(s)$ in (13a) and (13b). We are here at once confronted with all the problems familiar from the theory of the Riemann ζ-function: What is the distribution of the zeros of $\phi_{pp}(s)$? The critical strip is $0 \leqq \Re(s) \leqq k$; do all nontrivial zeros of $\phi_{pp}(s)$ lie on the middle line $\Re(s) = k/2$? In case $\phi_{pp}(s)$ belongs to a modular form with $c_0 = 0$ ("cusp form") we know a few facts. The function $\phi_{pp}(s)$ has no pole, of course, its series is absolutely convergent for $\Re(s) > (k+1)/2$, $\phi_{pp}(s)$ has no zeros on $\Re(s) = (k+1)/2$ but infinitely many ones on $\Re(s) = k/2$, results all due to R. A. Rankin [42]. Ramanujan has for $\phi_{pp}(s) = \Delta(1, \tau)$ made the conjecture $|\tau(p)| \leqq 2p^{11/2}$ and Petersson [34] has generalized it to

$$|\lambda_{pp}(p)| \leqq 2p^{(k-1)/2}$$

or, which is equivalent, to the conjecture that the quadratic equation $z^2 - \lambda_{pp}(p)z + p^{k-1} = 0$ (derived from the denominator in (13b) with $p^s = z$) does not have two different real roots, which, since $\lambda_{pp}(p)$ is real would mean that the roots have to be of absolute value $p^{(k-1)/2}$. This conjecture has a close similarity to Hasse's theorem which confirms the Riemann hypothesis for elliptic function fields over finite fields.

Hecke has extended his theory also to modular forms of level (Stufe) Q. The operators T_n with $(n, Q) = 1$ have the same behavior

as the operators for $Q=1$; the other ones, however. introduce complications on which I cannot dwell. Hecke applies this extension of his theory to a study of the ϑ-functions generated by quadratic forms of several variables [20].

So far I have spoken only of the theory of rational integers on one side and of functions of one variable on the other. I would overstep the limits which I had to set myself in this discussion if I were to enter upon the problems presented by the fields of algebraic numbers. In many respects a full analogy with the rational field can act as guide. However, some new features appear here, as, for example, the group of units. An algebraic field of degree n can be illustrated by an n-dimensional point lattice. Some problems, in particular additive ones, lead to analytic functions of n complex variables; some other problems, in particular the multiplicative ones, are handled by means of a set of ζ-functions with one complex variable s and $(n-1)$ integer parameters (Hecke's $\zeta(s, \lambda)$-functions) [15]. The multiplicative theory of algebraic fields is, through Hecke's fundamental investigations, about as far advanced as that for the rational field; the additive number theory in algebraic fields, however, is still in its beginnings.

The theory of quadratic forms offers another way to come to functions of several variables, as Siegel has recently shown in his introduction of modular functions of several variables [48].

This report could, of course, mention only selected topics of analytic number theory. I do not wish to imply that no recent progress has been made in subjects which I did not discuss. There are, for example, the important contributions to the estimates of lattice points in the circle and in other areas due to van der Corput and his successors, and the investigations of Siegel and Gelfond concerning the transcendentality of certain types of numbers. I have purposely chosen such portions of analytic number theory which seemed to me to exhibit most clearly the present tendency, the trend, in contemporary research work. Our discipline has grown beyond the stage of mere application of analysis to number theory; we can characterize the present tendency as a deep mutual penetration of analysis and arithmetic. It is still so that the theory of analytic functions helps to solve arithmetical problems which otherwise appear as inaccessible; but number theoretical problems are the sources of new functions, and number theoretical arguments lead to a deeper understanding of the structure of known functions. I think that analytic number theory is a branch of mathematics that fascinates through its harmony and beauty and appeals to the working mathematician through its variety and fruitfulness.

BIBLIOGRAPHY

1. E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, I, II, Mathematische Zeitschrift, vol. 19 (1924), pp. 153–206; 207–246.

2. S. Bochner and F. Bohnenblust, *Analytic functions with almost periodic coefficients*, Annals of Mathematics, (2), vol. 35 (1934), pp. 152–161.

3. Viggo Brun, *Le crible d'Eratosthène et le theorème de Goldbach*, Videnskapsselskapets Skrifter, Kristiania, 1920, no. 3.

4. H. Davenport, *On certain exponential sums*, Journal für die reine und angewandte Mathematik, vol. 169 (1933), pp. 158–176.

5. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, Journal für die reine und angewandte Mathematik, vol. 172 (1935), pp. 151–182.

6. L. E. Dickson, *Universal Waring theorems*, Monatshefte für Mathematik und Physik, vol. 43 (1936), pp. 391–400.

7. ———, *The ideal Waring theorem for twelfth powers*, Duke Mathematical Journal, vol. 2 (1936), pp. 192–204.

8. T. Estermann, *Proof that every large integer is the sum of two primes and a square*, Proceedings of the London Mathematical Society, (2), vol. 42 (1937), pp. 501–516.

9. Mary Haberzetle, *On some partition functions*, American Journal of Mathematics, vol. 63 (1941), pp. 589–599.

10. G. H. Hardy, *On the representation of a number as the sum of any number of squares, and in particular of five*, Transactions of this Society, vol. 21 (1920), pp. 255–284.

11. ———, *Ramanujan, Twelve Lectures on Subjects Suggested by His Life and Work*, Cambridge, 1940, 236 pp.

12. H. Hasse, *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen*, Göttinger Nachrichten, 1933, pp. 253–262.

13. ———, *Zur Theorie der abstrakten elliptischen Funktionenkörper*, I, II, III, Journal für die reine und angewandte Mathematik, vol. 175 (1936), pp. 55–62; 69–88; 193–208.

14. ———, *Über die Riemannsche Vermutung in Funktionenkörpern*, Comptes Rendus du Congrès International des Mathématiciens, Oslo, 1936, vol. 1, pp. 189–206.

15. E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen*, I, II, Mathematische Zeitschrift, vol. 1 (1918), pp. 357–376; vol. 6 (1920), pp. 11–51.

16. ———, *Die Primzahlen in der Theorie der elliptischen Modulfunktionen*, K. Danske Videnskabernes Selskab, Mathematisk-fysiske Meddelelser, vol. 13 (1935), 16 pp.

17. ———, *Neuere Fortschritte in der Theorie der elliptischen Modulfunktionen*, Comptes Rendus du Congrès International des Mathématiciens, Oslo, 1936, vol. 1, pp. 140–156.

18. ———, *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung*, I, II, Mathematische Annalen, vol. 114 (1937), pp. 1–28; 316–351.

19. ———, *Dirichlet series, modular functions and quadratic forms*, Lectures at the Institute for Advanced Study, Princeton, 1938, 48 pp.

20. ———, *Analytische Arithmetik der positiven quadratischen Formen*, K. Danske Videnskabernes Selskab, Mathematisk-fysiske Meddelelser, vol. 17 (1940), 134 pp.

21. Hans Heilbronn, *Über des Waringsche Problem*, Acta Arithmetica, vol. 1 (1936), pp. 212–221.

22. ———, *On the class-number of imaginary quadratic fields*, Quarterly Journal of Mathematics, Oxford, vol. 5 (1934), pp. 150–160.

23. L. K. Hua, *On the number of partitions of a number into unequal parts*, Transactions of this Society, vol. 51 (1942), pp. 194–201.

24. M. Kac, *Almost periodicity and the representation of integers as sums of squares*, American Journal of Mathematics, vol. 62 (1940), pp. 122–126.

25. M. Kac, E. R. van Kampen and Aurel Wintner, *Ramanujan sums and almost periodic functions*, American Journal of Mathematics, vol. 62 (1940), pp. 107–114.

26. D. H. Lehmer, *On a conjecture of Ramanujan*, Journal of the London Mathematical Society, vol. 11 (1936), pp. 114–118.

27. ———, *An application of Schläfli's modular equation to a conjecture of Ramanujan*, this Bulletin, vol. 44 (1938), pp. 84–90.

28. Joseph Lehner, *A partition function connected with the modulus five*, Duke Mathematical Journal, vol. 8 (1941), pp. 631–655.

29. L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions*, Proceedings of the Cambridge Philosophical Society, vol. 19 (1917), pp. 117–124.

30. ———, *Note on certain modular relations considered by Messrs. Ramanujan, Darling, and Rogers*, Proceedings of the London Mathematical Society, (2), vol. 20 (1922), pp. 408–416.

31. ———, *On a sum analogous to a Gauss sum*, Quarterly Journal of Mathematics, Oxford, vol. 3 (1932), pp. 161–167.

32. Ivan Niven, *On a certain partition function*, American Journal of Mathematics, vol. 62 (1940), pp. 353–364.

33. Hans Petersson, *Über die Entwicklungskoeffizienten der automorphen Formen* Acta Mathematica, vol. 58 (1932), pp. 169–215.

34. ———, *Konstruktion der sämtlichen Lösungen einer Riemannschen Funktionalgleichung durch Dirichlet-Reihen mit Eulerscher Produktentwicklung*, I, II, III, Mathematische Annalen, vol. 116 (1939), pp. 401–412; vol. 117 (1940), pp. 39–64; 277–300.

35. H. Rademacher, *A convergent series for the partition function $p(n)$*, Proceedings of the National Academy of Sciences, vol. 23 (1937), pp. 78–84.

36. ———, *On the partition function $p(n)$*, Proceedings of the London Mathematical Society, (2), vol. 43 (1937), pp. 241–254.

37. ———, *The Fourier coefficients of the modular invariant $J(\tau)$*, American Journal of Mathematics, vol. 60 (1938), pp. 501–512.

38. ———, *The Fourier series and the functional equation of the absolute modular invariant $J(\tau)$*, American Journal of Mathematics, vol. 61 (1939), pp. 237–248.

39. ———, *The Ramanujan identities under modular substitutions*, Transactions of this Society, vol. 51 (1942), pp. 609–636.

40. H. Rademacher and H. Zuckerman, *A new proof of two of Ramanujan's identities*, Annals of Mathematics, (2), vol. 40 (1939), pp. 473–489.

41. S. Ramanujan, *On certain arithmetical functions*, Transactions of the Cambridge Philosophical Society, vol. 22 (1916), pp. 159–184; also *Collected Papers*, pp. 136–162.

42. R. A. Rankin, *Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions*, I, II, III, Proceedings of the Cambridge Philosophical Society, vol. 35 (1939), pp. 351–356; 357–372; vol. 36 (1940), pp. 150–151.

43. H. Salié, *Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen*, Mathematische Zeitschrift, vol. 36 (1933), pp. 263–278.

44. F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Mathematische Zeitschrift, vol. 33 (1931), pp. 1–32.

45. B. Schoeneberg, *Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen*, Mathematische Annalen, vol. 116 (1939), pp. 511–523.

46. C. L. Siegel, *Über die Classenzahl quadratische Zahlkörper*, Acta Arithmetica, vol. 1 (1936), pp. 83–86.

47. ———, *Über die analytische Theorie der quadratischen Formen*, I, II, III, Annals of Mathematics, (2), vol. 36 (1935), pp. 527–606; vol. 37 (1936), pp. 230–263; vol. 38 (1937), pp. 212–291.

48. ———, *Einführung in die Theorie der Modulfunktionen n-ten Grades*, Mathematische Annalen, vol. 116 (1939), pp. 617–657.

49. N. Tchudakoff, *On zeros of Dirichlet's L-functions*, Recueil Mathématique (Matematicheskii Sbornik), vol. 43 (1936), pp. 591–601.

50. I. Vinogradoff, *On Waring's problem*, Annals of Mathematics, (2), vol. 36 (1935), pp. 395–405.

51. ———, *On Weyl's sums*, Recueil Mathématique (Matematicheskii Sbornik), vol. 42 (1935), pp. 521–530.

52. ———, *Representation of an odd number as a sum of three primes*, Comptes Rendus de l'Académie des Sciences de l'URSS (Doklady), vol. 15 (1937), pp. 169–172.

53. ———, *Some theorems concerning the theory of primes*, Recueil Mathématique (Matematicheskii Sbornik), vol. 44 (1937), pp. 179–195.

54. Arnold Walfisz, *Zur additiven Zahlentheorie*, IV, Travaux de l'Institut Mathématique de Tblissi, vol. 3 (1938), pp. 121–192.

55. G. N. Watson, *Ramanujans Vermutung über Zerfällungsanzahlen*, Journal für die reine und angewandte Mathematik, vol. 179 (1938), pp. 97–128.

56. André Weil, *Sur les fonctions algébriques à corps de constantes fini*, Comptes Rendus de l'Académie des Sciences, Paris, vol. 210 (1940), pp. 592–594.

57. ———, *On the Riemann hypothesis in function-fields*, Proceedings of the National Academy of Sciences, vol. 27 (1941), pp. 345–347.

58. Hermann Weyl, *Über die Gleichverteilung von Zahlen mod. Eins.*, Mathetische Annalen, vol. 77 (1916), pp. 313–352.

59. H. S. Zuckerman, *On the coefficients of certain modular forms belonging to subgroups of the modular group*, Transactions of this Society, vol. 45 (1939), pp. 298–321.

60. ———, *Identities analogous to Ramanujan's identities involving the partition function*, Duke Mathematical Journal, vol. 5 (1938), pp. 88–110.

UNIVERSITY OF PENNSYLVANIA

NORMAL VARIETIES AND BIRATIONAL CORRESPONDENCES

OSCAR ZARISKI

1. **Introduction.** As one advances into the general theory of algebraic varieties, one reluctantly but inevitably reaches the conclusion that there does not exist a general theory of birational correspondences. This may sound too reckless a statement or too harsh a criticism, especially if one thinks of the fundamental role which birational transformations are supposed to have in algebraic geometry. Nevertheless our conclusion is in exact agreement with the facts and it is made with constructive rather than with critical intentions. It is true that the geometers have a fairly good intuitive idea of what happens or what may happen to an algebraic variety when it undergoes a birational transformation; but the only thing they know with any certainty is what happens in a thousand and one special cases. All these special cases—and they include all Cremona transformations—are essentially reducible to one special but very important case, namely, the case in which the varieties under consideration are nonsingular(that is, free from singular points). One can give many reasons for regarding as inadequate any theory which has been developed exclusively for nonsingular varieties. One rather obvious reason is that we have as yet no proof that every variety of dimension greater than 3 can be transformed birationally into a nonsingular variety.[1] But there are other, less transient, reasons. Were such a proof available, it would still be advisable to develop the theory of algebraic varieties, *as far as possible*, without restricting oneself to nonsingular projective models. This certainly would be the correct program of work from an arithmetic standpoint. I have a distinct impression that my friends the algebraists have not much use anyway for the resolution of the singularities. All they want is a general uniformization theorem, and now that they have it, they are content.

The following consideration will perhaps carry greater weight with the geometers. It turns out, as I have found out at some cost to myself, that we have to know a lot more about birational correspondences than we know at present before we can even attempt to carry

An address delivered before the meeting of the Society in Bethlehem, Pa., on December 31, 1941, by invitation of the Program Committee; received by the editors January 22, 1942.

[1] The resolution of the singularities of three-dimensional varieties will be carried out in a forthcoming paper of mine.

out the resolution of the singularities of higher varieties. A general theory of birational correspondences is a necessary prerequisite for such an attempt. I shall have occasion later on to indicate some difficult questions concerning birational correspondences which arise in connection with the resolution of singularities.

2. **Birational correspondences and valuations.** From a formal point of view, there is nothing mysterious about a birational transformation. If $V = V_r^n$ is an irreducible r-dimensional algebraic variety in an n-dimensional projective space, the coordinates $\xi_1, \xi_2, \cdots, \xi_n$ of its general point are algebraic functions of r independent variables, and the field $\Sigma = K(\xi_1, \xi_2, \cdots, \xi_n)$ generated by these functions is *the field of rational functions on* V. Here K denotes the field of constants (in the classical case K is the field of complex numbers). If $V' = V_r'^m$ is another irreducible algebraic variety, with general point $(\xi_1', \xi_2', \cdots, \xi_m')$ and associated field $\Sigma' = K(\xi_1', \xi_2', \cdots, \xi_m')$, then the two varieties V and V' are *birationally equivalent* if the two fields Σ and Σ' are simply isomorphic: $\Sigma/K \cong \Sigma'/K$. A birational transformation is merely the process of passing from one variety to another, birationally equivalent, variety.

The difficulties begin when we wish to associate with this purely formal process a *geometric transformation*, that is, a correspondence between the points of the two varieties. From the equations of the transformation, in which the ξ''s are given as rational functions of the ξ's and vice versa, it is not difficult to conclude that the transformation sets up a (1, 1) correspondence between the non-special points of V and the non-special points of V'. The points of either variety for which the equations of the transformation fail to define corresponding points on the other variety are referred to as special points in the sense that they lie on certain algebraic subvarieties, of dimension less than r. In the classical case, considerations of continuity allow us to complete the definition of the correspondence also for these special points. In the abstract case we use valuation theory instead, as follows:

A *valuation* of the field Σ is an homomorphic mapping v of the multiplicative group $\Sigma - 0$ (that is, the element zero excluded) upon an ordered additive abelian group Γ, which satisfies the well known valuation axioms: (1) $v(\omega_1 \cdot \omega_2) = v(\omega_1) + v(\omega_2)$; (2) $v(\omega_1 \pm \omega_2) \geqq \min \{v(\omega_1), v(\omega_2)\}$; (3) $v(\omega) \neq 0$, for some ω in Σ; (4) $v(c) = 0$, for all constants $c \neq 0$. We put $v(0) = +\infty$.

In the case of algebraic functions of one variable, every valuation arises from a branch of our curve V. The value $v(\omega)$ is then *the order*

of ω at the branch and is an integer. Positive and negative $v(\omega)$ signify, respectively, that the center of the branch is a zero or a pole of the function ω, while if $v(\omega)=0$ then the function-theoretic value of ω at the center of the branch is a finite constant, different from zero. In this special case, it is clear that from an algebraic standpoint the function-theoretic values of the elements of the field are the cosets of the *valuation ring* $\mathfrak{B}$ $\{\omega\in\mathfrak{B}\leftrightarrow v(\omega)\geqq 0\}$, with respect to its subset consisting of the elements ω such that $v(\omega)>0$. This subset is a prime divisorless ideal $\mathfrak{p}$, and so the cosets form indeed a field; the field of complex numbers, in the classical case. This consideration is independent of the dimension of the field and can therefore be applied directly to the general case. It is therefore always possible to associate with any valuation v of Σ a mapping f of the elements of Σ upon the elements of another field (and the symbol ∞), *the field of residual classes* of $\mathfrak{B}$ mod $\mathfrak{p}$, and we may speak of $f(\omega)$, $\omega\in\Sigma$, as being the *function-theoretic value* of ω (if $v(\omega)<0$, then $f(\omega)=\infty$). This field is the so-called *residue field* of the valuation. However, if $r>1$ then the residue field may be a transcendental extension of the ground field K. Its degree of transcendence s over K, or briefly, *its dimension*, is at most $r-1$, and is referred to as the dimension of the valuation. A zero-dimensional valuation is called *a place* of the field Σ. The function-theoretic values of the elements of Σ at a given place are *constants*, that is, either elements of K or algebraic quantities over K.

Given a valuation v and a projective model V of Σ, with general point $(\xi_1, \xi_2, \cdots, \xi_n)$, it is permissible to assume that the function-theoretic values of the ξ's are different from ∞, since we may subject the coordinates ξ_i to an arbitrary projective transformation. Then the polynomials in the ξ's which have function-theoretic value zero form a prime ideal in the ring of all polynomials in the ξ's. This prime ideal defines an irreducible algebraic subvariety W of V. This subvariety W we call *the center of the valuation* v on the variety V. The dimension of W cannot exceed the dimension of the valuation. In particular, *the center of a place is always a point of* V.

The following geometric picture of a valuation is suggestive, although not entirely adequate. A zero-dimensional valuation, that is, a place, with center at a point P, corresponds to a way of approaching P along some one-dimensional branch, which may be algebraic, analytic, or transcendental. Similarly an s-dimensional valuation with an s-dimensional center W corresponds to a way of approaching W along an $(s+1)$-dimensional branch through W.

After these preliminaries, we define the birational correspondence between two birationally equivalent varieties V and V' as follows:

DEFINITION 1. *Two subvarieties W and W' of V and V', respectively, correspond to each other if there exists a valuation of the field Σ whose center on V is W and whose center on V' is W'.*

Note that our definition does not treat points in any privileged fashion. Any subvariety of V is treated as an element, rather than as a set of points. This procedure is much more convenient than the usual one in which corresponding loci are defined as loci of corresponding points.

In the study of the birational correspondence between V and V', it is found convenient to introduce a third variety $\overline{V}$ which is birationally related to both V and V', the so-called *join of V and V'* (or *the variety of pairs of corresponding points* of V and V'). $\overline{V}$ is defined as follows. We adjoin to Σ a new transcendental η_0 and we regard the $n+1$ quantities $\eta_0, \eta_1=\eta_0\xi_1, \cdots, \eta_n=\eta_0\xi_n$ as the *homogeneous coordinates* of the general point of V. Similarly, the $m+1$ quantities $\eta_0'=\eta_0, \eta_1'=\eta_0\xi_1', \cdots, \eta_m'=\eta_0\xi_m'$ will be the homogeneous coordinates of the general point of V'. The $(n+1)(m+1)$ quantities $\omega_{ij}=\eta_i\eta_j'$ can be regarded as the homogeneous coordinates of the general point of a variety birationally equivalent to V and to V'. This variety is our $\overline{V}$, the join of V and V'. The birational correspondence between $\overline{V}$ and V has the property that to any subvariety of $\overline{V}$ there corresponds a unique subvariety of V; in particular, to every point of $\overline{V}$ there corresponds a unique point of V. Similarly, for $\overline{V}$ and V'. Thus, both V and V' are single-valued transforms of $\overline{V}$. The properties of the birational correspondence between V and V' can be readily derived from the properties of the birational correspondences between $\overline{V}$ and V and between $\overline{V}$ and V'. We therefore replace one of the two varieties V, V', say V', by the join $\overline{V}$, that is, from now on we shall always assume that *V is a single-valued transform of V'*.

3. **Fundamental loci; geometric preliminaries.** On the basis of Definition 1, it is easy to prove that the points of V to which there correspond more than one point on V' constitute an algebraic subvariety F of V, and that every subvariety W of V to which there correspond more than one subvariety W' on V' must lie on F. This variety F is called the *fundamental locus* of the birational correspondence, and every W which lies on F is a *fundamental* variety. This is not our final definition, but it will do for the moment. Note that the fundamental locus on V' is an empty set, in view of our assumption that V is a single-valued transform of V'.

What corresponds on V' to a fundamental variety W of V? To this question we have a complete answer in the case of a nonsingular

V. We have, namely, in this case the following two fundamental theorems (see van der Waerden, *Algebraische Korrespondenzen und rationale Abbildungen*, Mathematische Annalen, vol. 110 (1934)):

A. *If W is an irreducible s-dimensional fundamental variety of V, then the transform of W is an algebraic subvariety of V' whose irreducible components are all of dimension greater than s.*

B. *The transform of the fundamental locus F is a pure $(r-1)$-dimensional subvariety of V'.*

The following examples show that both theorems fail to hold for singular models.

(1) If P is a point of V at which V is *locally reducible*, that is, if in the neighborhood of P the variety V consists of ν ($\nu>1$) analytical r-dimensional branches, then in *special cases* it turns out that V is the projection of another variety V' on which these ν branches become separated.[2] Then the point P will be the projection of ν distinct points of V', and this contradicts Theorem A.

(2) Let Q be a ruled quadric surface in S_3 and let V be the three-dimensional cone which projects Q from a point O not in S_3. We take another copy of Q, say Q', which we now imagine as being immersed in an S_5. Let l be a line in S_5 which does not meet the S_3 containing the quadric. We set up a (1, 1) projective correspondence between the points P' of l and the lines p of one ruling of the quadric. Let V' be the irreducible three-dimensional variety generated by the planes (P', p), where P' and p are corresponding elements in the above projectivity. It is easy to set up a birational correspondence between V and V' in which to the planes (O, p) there correspond the planes (P', p). There will be no fundamental points on V', while O will be the only fundamental point on V. To the point O there corresponds on V' the line l, in contradiction with Theorem B.

One has the feeling that the second example does more damage than the first, because the first counterexample could be explained away on the basis that the point P, as origin of ν analytical branches, should not be regarded at all as a "point" of the variety, but rather as a point of the ambient projective space at which ν "points" of the variety accidentally happened to come together. This explanation, if stripped of all metaphysics, can have only one mathematical meaning, namely, it means, by implication, that in the general theory of birational correspondence, we should restrict ourselves to varieties

[2] Whether this is true generally, is not at all obvious and, in fact, has never been proved.

which are locally irreducible at each point. What interests us in this argument is the formal admission that some kind of restriction as to the type of varieties to be studied is necessary in the theory of birational correspondences. Whether or not the restriction to locally irreducible varieties is the right one, is a debatable matter. For one thing, it is not certain that in making such a restriction we are not being too stingy, unless we can prove that the branches of a variety can always be separated by the method of projection. This is probably true and should not be too difficult to prove. Actually we regard this restriction as being too generous. For, besides the requirement that the varieties V of our hypothetical restricted class satisfy Theorem A, we find it essential that these varieties also satisfy the following additional condition:

C. *If to a point P of V there corresponds a unique point P' of V', then the birational correspondence, regarded as an analytical transformation, is regular at P.*

The geometric meaning of this condition can be roughly indicated as follows. If this condition and condition A are satisfied for a given variety V, then the analytical structure of the neighborhood of any point P of V cannot be affected by a birational transformation, unless this transformation blows up P into a curve, or a surface and so on (always provided we replace the transform V' of V by the join $\overline{V}$; compare with §2). In particular, it is not possible to simplify any further the type of singularity which V possesses at P without doing a thing as radical as that of spreading out that singular point into a variety of dimension greater than 0. From this point of view, condition C can be looked upon as a sort of maximality condition.

In the case of algebraic curves it follows readily from this geometric interpretation that the only curves which satisfy conditions A and C are the nonsingular curves. But already in the case of surfaces we get a much wider variety of types. For instance, it can be proved that the surfaces in S_3 which satisfy our conditions are the surfaces which have only isolated singularities.

We now proceed to define arithmetically the varieties of our restricted class. We call these varieties *locally normal*. Included among these varieties are those which I have called *normal* varieties. The algebraic operation which plays a fundamental role in our arithmetic approach to the geometric questions just outlined is that of the *integral closure of a ring in its quotient field*. Theorem C follows in a relatively simple fashion from our arithmetic definitions and from some well known theorems in valuation theory. Theorem A lies much

deeper and its proof is more difficult. As to Theorem B, it definitely must be sacrificed when we are dealing with singular varieties.

4. **Locally normal and normal varieties.** We use the homogeneous coordinates $\eta_0, \eta_1, \cdots, \eta_n$ of the general point of V (§2) and we define the *quotient ring* $Q(P)$ of any point P of V as the ring of all quotients $f(\eta)/g(\eta)$, where f and g are forms of like degree in $\eta_0, \eta_1, \cdots, \eta_n$ and where $g \neq 0$ at P. In other words, the quotient ring $Q(P)$ consists of all functions in our field Σ which have a definite and finite value at P. In a similar fashion, we define the quotient ring $Q(W)$ of any irreducible algebraic subvariety W of V by the condition that $g(\eta) \not\equiv 0$ on W (that is, that g should not vanish at every point of W).

One is led to the consideration of quotient rings when one examines the equations of a birational correspondence between V and another variety V'. For it is seen immediately that if the nonhomogeneous coordinates $\xi_1', \cdots, \xi_m'$ of the general point of V' belong to the quotient ring $Q(W)$ of a given W on V, then to W there corresponds a unique subvariety W' on V' and moreover $Q(W')$ will be a subring of $Q(W)$. If $Q(W') = Q(W)$, then also W will be the only subvariety of V which corresponds to W'. In this case we say that the birational correspondence is *regular at* W, or *along* W. In particular, if the birational correspondence is regular at a point P of V, then as an analytical transformation it is regular in the neighborhood of P. Therefore, the quotient ring of a point determines uniquely the analytical structure of the neighborhood of the point. In the sequel we shall say that a birational correspondence is *regular* on V if it is regular at each point of V.

DEFINITION 2. *A variety V is locally normal along a subvariety W, if the quotient ring $Q(W)$ is integrally closed in its quotient field (that is, in Σ).*

DEFINITION 3. *V is locally normal, if it is locally normal at each point.*

The last definition refers only to points. The reason for this is the following: If V is locally normal at one point P of a subvariety W of V, then it is also locally normal along W. Hence if V is locally normal, in the sense of Definition 3, it is also locally normal along any W.

It is not difficult to show that V is locally normal if and only if the following condition is satisfied: *If $\mathfrak{C}$ is the conductor of the ring $K[\eta_0, \eta_1, \cdots, \eta_n]$ with respect to the integral closure of this ring in its quotient field, then the subvariety of V determined by the (homogeneous) ideal $\mathfrak{C}$ is empty.* This implies that either $\mathfrak{C}$ has no zeros at all, or its only zero is the trivial one: $(0, 0, \cdots, 0)$. Therefore, $\mathfrak{C}$ is either

the unit ideal or is a primary ideal belonging to the irrelevant prime ideal $(\eta_0, \eta_1, \cdots, \eta_n)$.

If $\mathfrak{C}$ is the unit ideal, we say that V is *normal*, that is, we give the following definition:

DEFINITION 4. *A variety V is normal if the ring $K[\eta_0, \eta_1, \cdots, \eta_n]$ is integrally closed in its quotient field.*

It can be proved that the singular manifold of a locally normal r-dimensional variety is of dimension less than or equal to $r-2$ (in particular, *a locally normal curve is nonsingular*). The converse is not generally true, except in the case $r=1$, *since a nonsingular curve is always locally normal.* However, *the converse is true for hypersurfaces*, that is, for V_r's in an S_{r+1}, Thus any surface in S_3 is locally normal if and only if it has a finite number of singularities.

It is important to point out that *nonsingular varieties are always locally normal.*

Our definitions clearly indicate that normal varieties can differ from locally normal varieties only by some property at large, since locally they cannot be distinguished from each other. This difference at large is put into evidence by the following characterization of normal varieties, due to Muhly: *A variety V is normal if and only if the hypersurfaces of its ambient space, of any given order m, cut out on V a complete linear system.* Now it can be proved that locally normal varieties are characterized by the completeness of the above linear systems *for sufficiently high values of m.* This last result, in conjunction with the fact that every nonsingular V is locally normal, contains as a special case of the well known lemma of Castelnuovo concerning nonsingular curves. This lemma plays an important role in Severi's proof of Riemann-Roch's theorem for surfaces.

We have already pointed out that for locally normal varieties Theorems A and C hold true. Moreover it can be shown that these are the only varieties for which these theorems are true. It may be added that there is really no great loss of generality in confining the theory of birational correspondences to locally normal varieties. For it can be shown that any variety V determines uniquely, *to within regular birational transformations*, a locally normal variety V' which is birationally equivalent to V and which is such that: (a) to each point P' of V' there corresponds a unique point P of V, and we have always: $Q(P') \supseteq Q(P)$; (b) to any point P of V there corresponds a finite number of points on V'; (c) if V is locally normal at P, then the birational correspondence between V and V' is regular at P. It is not difficult to show that these properties of the birational correspondence between

V and V' imply that, to within a regular birational transformation, *V is the projection of V' from a center S_k which does not meet V'.*

It would be of interest to characterize the locally normal varieties for which Theorem B holds. It can be proved that the following condition is sufficient for the validity of Theorem B: If P is any point of V and if W is any $(r-1)$-dimensional subvariety through P, then a sufficiently high multiple of W should be *locally* (that is, at P) complete intersection of V with an hypersurface of the ambient space. In terms of ideal theory, this means that in the quotient ring of P a sufficiently high power of any minimal prime ideal should be *quasi-gleich* (in the sense of van der Waerden) to a principal ideal. This condition gives us a good insight into the "real" reason of the validity of Theorem B for nonsingular varieties; for we know that if P is a simple point, then every minimal prime ideal in $Q(P)$ is itself a principal ideal.

5. **Monoidal transformations.** I should now like to discuss briefly a special class of birational correspondences which seem to be very useful in the theory of singularities, whether we deal with the resolution of singularities or with the analysis of the composition of a singularity from the standpoint of infinitely near points. These special transformations are the hyperspace analogue of plane quadratic transformations, and they are therefore of importance also for the general theory of birational correspondences.

When we are dealing with locally normal varieties V, we find it most convenient to define fundamental varieties of a birational correspondence between V and another variety V', as follows:

DEFINITION 5. *An irreducible subvariety W of V is fundamental if a corresponding subvariety W' of V' exists such that $Q(W) \not\supseteq Q(W')$.*

We know from §4 that if $Q(W) \supseteq Q(W')$, then W' is the only subvariety which corresponds to W. Hence if W is fundamental, then the relation $Q(W) \not\supseteq Q(W')$ is true for any W' which corresponds to W. If the birational correspondence has no fundamental points on V and on V', then $Q(W) = Q(W')$, for *any* two corresponding subvarieties W and W', and the transformation is regular on V (and on V'). We do not regard two birational transformations as being essentially distinct if they differ only by a regular birational transformation.

We consider a birational correspondence between two locally normal varieties V and V', and we again restrict ourselves to the case in which the given correspondence has no fundamental points on V'. Then V' is in regular birational correspondence with the join $\overline{V}$ of V'

and V, and we may replace V' by $\overline{V}$. Consequently, we assume that the equations of the birational correspondence between V and V' are of the form:

$$\rho\eta_{ij} = \eta_i\phi_j, \qquad i = 0, 1, \cdots, n; j = 0, 1, \cdots, m,$$

where $\eta_0, \eta_1, \cdots, \eta_n$ are the homogeneous coordinates of the general point of V and where the ϕ_j are forms of like degree in the η's. Here ρ is a factor of proportionality and the η_{ij} are the homogeneous coordinates of the general point of V'. It can be shown that the fundamental locus on V is given by the base manifold of the *linear system* $\lambda_0\phi_0 + \cdots + \lambda_m\phi_m = 0$, provided we first drop all fixed $(r-1)$-dimensional components of the system. In terms of ideal theory, it means that we first write each principal ideal (ϕ_j) as a power product of minimal primes, say $(\phi_j) = \mathfrak{A}\mathfrak{B}_j$, where $\mathfrak{A}$ is the highest common divisor of $(\phi_0), \cdots, (\phi_m)$. Then the fundamental locus is given by the ideal $(\mathfrak{B}_0, \mathfrak{B}_1, \cdots, \mathfrak{B}_m)$. This ideal is of dimension less than or equal to $r-2$.

The special transformations which we wish to discuss are those for which $(\phi_0, \phi_1, \cdots, \phi_m)$ is itself a prime ideal, of dimension $s \leqq r-2$ or differs from a prime ideal by an irrelevant primary component. For the lack of a better name, we call them *monoidal transformations*.[3] The irreducible subvariety W of V defined by the ideal $(\phi_0, \phi_1, \cdots, \phi_m)$ is called the *center* of the transformation. It is not difficult to see that a change of the base of the ideal $(\phi_0, \cdots, \phi_m)$ does not essentially affect the transformation. A *quadratic transformation* is a special case of a monoidal transformation, the center is in that case a point.

The effect of a monoidal transformation consists in that the center W is spread out into an $(r-1)$-dimensional irreducible subvariety W' of V'. Moreover, *points of W which are simple both for V and W, correspond to simple points of W'*. This is the main reason why a monoidal transformation is a useful tool in the resolution of singularities, since while it may conceivably simplify some singular points which lie on its center, it does not introduce new singularities.[4]

There are two outstanding problems concerning monoidal trans-

[3] With some non-essential modifications, and without their projective trimmings, the space Cremona transformations, known as monoidal transformations, are monoidal transformations in our sense.

[4] There is one exception: to a simple point of V which is *singular* for W there may correspond singular points of V'! For this reason it is usually advisable to "smooth out" W, that is, to resolve the singularities of W, before one applies the monoidal transformation.

formations which play a role in the problem of resolution of singularities, but which at the same time are decisively of interest in themselves. We proceed to outline these questions.

PROBLEM 1. *Given any birational correspondence between two nonsingular models V and V', and assuming that there are no fundamental points on V', show that the birational transformation can be decomposed into monoidal transformations.*

In other words, the question is to show that for nonsingular models the monoidal transformations form a set of generators of the birational group. It is very likely that this decomposition exists also when only V' is nonsingular.

PROBLEM 2. *Given any birational correspondence between two arbitrary (not necessarily nonsingular) models V and V', and assuming as before that there are no fundamental points on V', show that the fundamental varieties on V can be eliminated by monoidal transformations.*

By this I mean that it is asked to transform V by a sequence of monoidal transformations into another variety V^* such that the birational correspondence between V^* and V' has no fundamental points on V^*.

As to Problem 1, we have a proof in the case of surfaces. In this case, the result can be regarded as a generalization of the well known theorem of Noether on the decomposition of plane Cremona transformations into quadratic transformations, although Noether's theorem is not a special case of this general result. It may be well to clarify the connection between the two results. In the first place, a quadratic Cremona transformation is not at all a quadratic transformation in our sense. Our quadratic transformation has only one ordinary fundamental point, and its inverse has no fundamental points at all, while a plane quadratic transformation and its inverse both have three fundamental points, which in special cases may be infinitely near points. For this reason a plane Cremona transformation can never be a quadratic transformation in our sense. The transform of a plane π under a quadratic transformation in our sense is not a plane, but a certain rational surface M in S_5, or any other surface in regular birational correspondence with M. Of course, an ordinary quadratic transformation between two planes π and π' can be expressed as a product of quadratic transformations in our sense, or more precisely as the product of 3 successive quadratic transformations and of 3 inverses of quadratic transformations. Since our proof takes care of surfaces over abstract fields K, it yields immediately a

corresponding result for the fundamental varieties W of dimension $r-2$ in the general case, for the adjunction of certain $r-2$ transcendentals to the ground field will make a surface out of the variety V and a point out of W. In particular, the decomposition into monoidal transformations is thus established for birational correspondences between nonsingular three-dimensional varieties, provided the correspondence has only fundamental curves, but no isolated fundamental points.

In applications of Problem 2, the main interest lies in the elimination of the *simple* fundamental varieties of V. In this case we have a complete proof, provided the resolution theorem is granted for varieties of *dimension two less* than the dimension of V. Thus, in the case of three-dimensional varieties we have to use only a thing as little as that of the resolution of singularities of an algebraic curve. It is clear that Problem 2 is to be viewed as a step in an inductive proof of the general theorem of the resolution of singularities rather than as a problem for the solution of which we first need that general theorem. The really important problem is Problem 1. Its solution seems to be essential for the resolution of singularities of higher varieties. Thus, it is possible to carry out the resolution of singularities of three-dimensional varieties, because we have the theorem of local uniformization for the varieties of this dimension, plus the solution of Problem 1 for surfaces over abstract fields of constants.

THE JOHNS HOPKINS UNIVERSITY

ON DIFFERENTIATION OF INTEGRALS AND APPROXIMATE CONTINUITY

ARTHUR ROSENTHAL

The following discussion is closely connected with Lebesgue's theorem that the derivative of an integral is equal to the integrand almost everywhere. It is well known that in generalizing this theorem to higher dimensions, great care must be exercised in the choice of the systems of intervals or sets used for n-dimensional differentiation.

Lebesgue[1] had already observed that arbitrary intervals (parallel to the axes) cannot be used for the generalization of that theorem, but only such intervals whose edges have a bounded ratio, or, more generally, such sets which are *regular* relative to the cubes. This also corresponds to the behavior of the most essential tool used in the proof, namely, Vitali's covering theorem. Saks[2] and, independently, Busemann and Feller[3] found later that there is a remarkable difference between the integrals of bounded[4] and unbounded functions: in the first (but not generally in the last) case, differentiation relative to arbitrary intervals (parallel to the axes) furnishes the integrand almost everywhere. But, according to Zygmund and Nikodym[5] and to Busemann and Feller,[3] even in the case of bounded integrands, differentiation relative to the system of all rectangular parallelopipeds (arbitrarily oriented) does not always furnish the integrand almost everywhere.

As to integrals in abstract spaces—in the case of bounded integrands, de Possel[6] gave necessary and sufficient conditions for the systems of sets used in differentiation to permit a generalization of Lebesgue's theorem; while in case of arbitrary integrands, de Possel[6]

Presented to the Society, September 5, 1941; received by the editors July 14, 1941.

[1] H. Lebesgue, Annales de l'École Normale, (3), vol. 27 (1910), pp. 363, 387.

[2] S. Saks, *Théorie de l'Intégrale*, Warsaw, 1933, p. 232; *Theory of the Integral*, Warsaw, Lwow, 1937, p. 132.

[3] H. Busemann and W. Feller, Fundamenta Mathematicae, vol. 22 (1934), pp. 226–256.

[4] Further generalizations: A. Zygmund, Fundamenta Mathematicae, vol. 23 (1934), pp. 143–149; B. Jessen, J. Marcinkiewicz, A. Zygmund, Fundamenta Mathematicae, vol. 25 (1935), pp. 217–234.

[5] O. Nikodym, Fundamenta Mathematicae, vol. 10 (1927), pp. 167–168 (note cf. A. Zygmund).

[6] R. de Possel, Comptes Rendus de l'Académie des Sciences, Paris, vol. 201 (1935), pp. 579–581; Journal de Mathématiques, (9), vol. 15 (1936), pp. 391–409.

and Hahn (in a still unpublished manuscript[7]) gave sufficient conditions suggested by Vitali's covering theorem.

On the other hand, in the case of bounded integrands, the original result of Lebesgue has been supplemented in an essential way by a theorem of Denjoy,[8] namely, that differentiation of an integral furnishes the integrand certainly wherever the integrand is *approximately continuous*. Denjoy proved this theorem for the case of one dimension, Saks[2] generalized it for more dimensions, namely—as in Lebesgue's theorem for bounded functions—using arbitrary intervals. Of course, the definition of approximate continuity depends on the notion of the density of a set M, and as the density of M results from differentiation of the characteristic function of M, the notion of approximate continuity also depends on the systems of sets used for this differentiation. Therefore, it is natural to use the same systems for definition of density and consequently of approximate continuity as for differentiation of the integral, especially if we are speaking (as in the theorem of Denjoy) about approximate continuity and differentiation simultaneously.

In preparing the second volume of Hahn's *Reelle Funktionen*,[7] I observed that there is an essential difference between the generalization of Lebesgue's theorem and that of Denjoy: While in the case of *Lebesgue's* theorem (also for bounded integrands) only rather *special* systems of sets can be used for differentiation, it is possible for the generalization of *Denjoy's* theorem, in any metric space (as will be shown), to *differentiate relative to quite arbitrary*, only *indefinitely fine, systems of sets* (see Theorem 1).[9] In a certain sense (namely, for *regular* derivatives), the approximate continuity at a point is even *necessary and sufficient* for the derivative of the integral to be equal to the integrand, assumed as bounded (see Theorem 4).

Another theorem of Denjoy[10] states that every measurable function is approximately continuous almost everywhere. The systems of sets

---

[7] This manuscript forms the basis of the second volume of Hahn's *Reelle Funktionen* which is now being elaborated and prepared for publication by the author of the present paper. The more general systems used by de Possel (see Footnote 6) in the case of bounded integrands, or the quite arbitrary "indefinitely fine" systems to be used here, had not been considered by Hahn. The notations of this second volume are used here.

[8] A. Denjoy, *Sur les fonctions dérivées sommables*, Bulletin de la Société Mathématique de France, vol. 43 (1915), p. 172.

[9] For instance, in the n-space relative to the system of all the rectangular parallelopipeds (arbitrarily oriented).

[10] A. Denjoy, loc. cit., p. 170; see also W. Sierpinski, Fundamenta Mathematicae, vol. 3 (1922), p. 320.

used in the generalization of this theorem can be the same[11] as, but cannot be more general than, those used in the generalization of Lebesgue's theorem for bounded integrands, for the two theorems of Denjoy taken together immediately imply Lebesgue's theorem for bounded integrands.

Thus we have the following situation: For the generalization of Denjoy's theorem that the derivative of an integral furnishes the integrand (assumed as bounded) certainly wherever the integrand is approximately continuous, the systems of sets used for differentiation can be chosen quite arbitrarily; yet in order to get Lebesgue's result that the integrand is obtained almost everywhere (or Denjoy's second result that the integrand is approximately continuous almost everywhere), the systems of sets employed must be rather special.

Let R be a metric space, $\mathfrak{M}$ a σ-field consisting of subsets of R, with $R \in \mathfrak{M}$; let ϕ and ψ be totally additive, finite set functions in $\mathfrak{M}$; let $\psi(M) \geqq 0$ for $M \in \mathfrak{M}$, (so that $\psi(M)$ is monotone increasing in $\mathfrak{M}$), and let $\mathfrak{M}$ be complete for ψ.

A system $\mathfrak{Q} \subseteq \mathfrak{M}$ of sets may be called an *indefinitely fine system of sets*, if to every point $a \in R$ there corresponds a certain subsystem $\mathfrak{Q}_a \subseteq \mathfrak{Q}$ consisting of non-empty sets such that for every $\rho > 0$ there is a set $Q \in \mathfrak{Q}_a$ contained in the sphere $S_{a\rho}$ (with center a and radius ρ).

If there is a sequence of sets $Q_\nu \in \mathfrak{Q}_a$ converging to a so that the sequence[12] $\phi(Q_\nu)/\psi(Q_\nu)$ converges to a limit d,[13] then d will be called a *derivate* of ϕ with respect to ψ at the point a relative to $\mathfrak{Q}$. The largest and smallest of these numbers d[13] (if a is fixed) are called the *upper* and *lower derivate* of ϕ with respect to ψ at a relative to $\mathfrak{Q}$:

$$\overline{D}(a, \phi, \psi, \mathfrak{Q}), \qquad \underline{D}(a, \phi, \psi, \mathfrak{Q}).$$

If

$$\overline{D}(a, \phi, \psi, \mathfrak{Q}) = \underline{D}(a, \phi, \psi, \mathfrak{Q}),$$

we call this value the *derivative* $D(a, \phi, \psi, \mathfrak{Q})$ of ϕ with respect to ψ at a relative to $\mathfrak{Q}$.

Following Lebesgue[1] we say that a sequence of sets $M_\nu \in \mathfrak{M}$ *converges regularly* to a (for ψ relative to $\mathfrak{Q}$), if there exists a number $\zeta(a) > 0$ and a sequence of sets $Q_\nu \in \mathfrak{Q}_a$ converging to a, such that for almost all ν we have:

---

[11] We shall not prove it here.

[12] If $\psi(Q_\nu) = 0$, this quotient is to be $0, +\infty, -\infty$, according as $\phi(Q_\nu) = 0, > 0, < 0$.

[13] Which may be finite or infinite.

(1) $$M_\nu \subseteq Q_\nu, \qquad \psi(M_\nu) \geqq \zeta \cdot \psi(Q_\nu).$$

If we have $\phi(M_\nu)/\psi(M_\nu) \to D(a, \phi, \psi, \mathfrak{Q})$ for every sequence M_ν converging regularly to a (for ψ relative to $\mathfrak{Q}$), we say that the *derivative* $D(a, \phi, \psi, \mathfrak{Q})$ is *regular* at a.

If $A \in \mathfrak{M}$, let us set $\phi(M) = \psi(AM)$; then $\overline{D}(a, \phi, \psi, \mathfrak{Q})$, $\underline{D}(a, \phi, \psi, \mathfrak{Q})$, and $D(a, \phi, \psi, \mathfrak{Q})$ become the *upper density* $\bar{d}(a, A, \psi, \mathfrak{Q})$, the *lower density* $\underline{d}(a, A, \psi, \mathfrak{Q})$, and the *density* $d(a, A, \psi, \mathfrak{Q})$ of A at a for ψ relative to $\mathfrak{Q}$; all these values are greater than or equal to 0 and less then or equal to 1.

Let R^* be the set of all those $a \in R$ for which there is a sequence of sets $Q_\nu \in \mathfrak{Q}_a$ converging to a, such that $\psi(Q_\nu) = 0$. Then we have:

(2) $$\underline{d}(a, A, \psi, \mathfrak{Q}) = 0, \qquad \text{for all } a \in R^*.$$

LEMMA 1. *For every $a \in R - R^*$ we have:*

$$\underline{d}(a, A, \psi, \mathfrak{Q}) + \bar{d}(a, R - A, \psi, \mathfrak{Q}) = 1;$$

$$\bar{d}(a, A, \psi, \mathfrak{Q}) + \underline{d}(a, R - A, \psi, \mathfrak{Q}) = 1.$$

PROOF. If $Q \in \mathfrak{Q}_a$, then $\psi(AQ) + \psi((R-A)Q) = \psi(Q)$; thus, if $\psi(Q) \neq 0$: $\psi(AQ)/\psi(Q) + \psi((R-A)Q)/\psi(Q) = 1$.

LEMMA 2. *If $d(a, A_1, \psi, \mathfrak{Q}) = 0$ and $d(a, A_2, \psi, \mathfrak{Q}) = 0$, then also $d(a, A_1 + A_2, \psi, \mathfrak{Q}) = 0$.*

PROOF. Let $Q_\nu \in \mathfrak{Q}_a$ be a sequence converging to a and choose $\epsilon > 0$; then $\psi(A_1 Q_\nu) \leqq \epsilon\psi(Q_\nu)$, $\psi(A_2 Q_\nu) \leqq \epsilon\psi(Q_\nu)$ for almost all ν; thus also $\psi((A_1 + A_2)Q_\nu) \leqq 2\epsilon\psi(Q_\nu)$, that is, $\psi((A_1 + A_2)Q_\nu)/\psi(Q_\nu) \to 0$.

LEMMA 3. *If $d(a, A_1, \psi, \mathfrak{Q}) = 1$ and $d(a, A_2, \psi, \mathfrak{Q}) = 1$, then also $d(a, A_1 A_2, \psi, \mathfrak{Q}) = 1$.*

PROOF. According to (2): $a \in R - R^*$; therefore because of Lemma 1, $d(a, R - A_1, \psi, \mathfrak{Q}) = 0$, $d(a, R - A_2, \psi, \mathfrak{Q}) = 0$, which implies by Lemma 2, $d(a, R - A_1 A_2, \psi, \mathfrak{Q}) = 0$; therefore again because of Lemma 1, $d(a, A_1 A_2, \psi, \mathfrak{Q}) = 1$.

If α, β are two real numbers ($\pm\infty$ permitted), we write:[14] $\|\alpha - \beta\| = |S(\alpha) - S(\beta)|$, where $S(\xi)$ means the "bounding transformation" $\xi/(1 + |\xi|)$. Furthermore, $[f(x) < y]$ denotes the set of all $x \in R$, for which $f(x) < y$ holds; similar notations are used in analogous cases.

In the following, let f always be a *ψ-measurable* function (that is, measurable with respect to ψ as measure).

[14] H. Hahn, *Reelle Funktionen*, I, Leipzig, 1932, p. 178.

The function f is called *approximately continuous*[15] at the point a (for ψ relative to $\mathfrak{Q}$), if for every $\epsilon>0$ the set $[\|f(x)-f(a)\|<\epsilon]$ has density 1 at a (for ψ relative to $\mathfrak{Q}$). If $f(a)$ is finite, in this definition $\|f(x)-f(a)\|<\epsilon$ may be replaced by $|f(x)-f(a)|<\epsilon$.

Equation (2) immediately implies the following lemma.

LEMMA 4. *If f is approximately continuous at a (for ψ relative to $\mathfrak{Q}$), then $a\in R-R^*$.*

LEMMA 5.[16] *In order that f be approximately continuous at a (for ψ relative to $\mathfrak{Q}$), it is necessary and sufficient that for every $y>f(a)$ and for every $y'<f(a)$ the sets $[f(x)<y]$ and $[f(x)>y']$ have density 1 at a (for ψ relative to $\mathfrak{Q}$).*

NECESSITY. Let $\epsilon>0$ be sufficiently small; then $y>f(a)$, $y'<f(a)$ imply $[\|f(x)-f(a)\|<\epsilon]\subseteq[f(x)<y]$ and $\subseteq[f(x)>y']$.

SUFFICIENCY. If for every $y>f(a)$ and every $y'<f(a)$ the sets $[f(x)<y]$ and $[f(x)>y']$ have density 1 at a, then, because of Lemma 3, the same is true for the set $[f(x)<y]\cdot[f(x)>y']$ and thus also for the set $[\|f(x)-f(a)\|<\epsilon]$.

LEMMA 6. *In order that f be not approximately continuous at the point $a\in R-R^*$ (for ψ relative to $\mathfrak{Q}$), it is necessary and sufficient that there exists either a $y>f(a)$ or a $y'<f(a)$, so that the upper density (for ψ relative to $\mathfrak{Q}$) of the set $[f(x)\geqq y]$ or $[f(x)\leqq y']$ is positive at a.*

NECESSITY. Because of Lemma 5, there exists either a $y>f(a)$ or a $y'<f(a)$, such that the set $[f(x)<y]=A$ or $[f(x)>y']=A'$ has a lower density less than 1 at a. But $R-A=[f(x)\geqq y]$, $R-A'=[f(x)\leqq y']$, and, because of Lemma 1, we have either $\bar{d}(a, R-A, \psi, \mathfrak{Q})>0$ or $\bar{d}(a, R-A', \psi, \mathfrak{Q})>0$.

SUFFICIENCY. Using the same notation, we have either $\bar{d}(a, R-A, \psi, \mathfrak{Q})>0$ or $\bar{d}(a, R-A', \psi, \mathfrak{Q})>0$. Thus because of Lemma 1, either

$$\underline{d}(a, A, \psi, \mathfrak{Q})<1$$

or

$$\underline{d}(a, A', \psi, \mathfrak{Q})<1.$$

Therefore, because of Lemma 5, f is not approximately continuous at a.

[15] A. Denjoy, loc. cit., p. 165.

[16] A. Denjoy, loc. cit., p. 169.

LEMMA 7. *If $|f| \leqq k$ holds, except perhaps on a set of ψ-measure zero, and if f is approximately continuous at a, then also $|f(a)| \leqq k$.*

PROOF. We set $[f(x) > k] = A$; then $\psi(A) = 0$. If $f(a) > k$, then, according to Lemma 5, A has density 1 at a; thus there exists a set $Q \in \mathfrak{Q}_a$, such that $\psi(AQ) > 0$; therefore we have $\psi(A) > 0$, contrary to $\psi(A) = 0$. In the same way we see that $f(a) < -k$ is impossible.

Now let the function f be not only ψ-measurable in R, but also *ψ-integrable* (that is, integrable with respect to the measure ψ) for all $M \in \mathfrak{M}$ in the sense of Radon and Fréchet;[17] we set $\phi(M) = (M)\int f d\psi$, where f is integrated with respect to ψ over the set $M \in \mathfrak{M}$. If the ψ-measurable function f is *ψ-bounded* (that is, bounded, except perhaps on a set of ψ-measure zero), then f is also ψ-integrable.

THEOREM 1. *Let $\mathfrak{Q}$ be an indefinitely fine system, let f be ψ-measurable and ψ-bounded*[18] *in R, and $\phi(M) = (M)\int f d\psi$. If f is approximately continuous at a for ψ relative to $\mathfrak{Q}$, then ϕ has the derivative $D(a, \phi, \psi, \mathfrak{Q}) = f(a)$ at a.*

PROOF. Let $Q_\nu \in \mathfrak{Q}_a$ be a sequence of sets converging to a. As we have $a \in R - R^*$ according to Lemma 4, we can assume $\psi(Q_\nu) \neq 0$. As f is ψ-bounded, because of Lemma 7 $f(a)$ is finite. For a given $\epsilon > 0$, we write: $B = [|f(x) - f(a)| < \epsilon]$. Then we have

$$\phi(Q_\nu) = (Q_\nu B)\int f d\psi + (Q_\nu - B)\int f d\psi. \tag{3}$$

Because of $|f(x) - f(a)| < \epsilon$ on B, we have

$$(Q_\nu B)\int f d\psi = (f(a) + \theta_1 \epsilon)\cdot\psi(Q_\nu B), \qquad |\theta_1| \leqq 1. \tag{4}$$

As f is ψ-bounded, there is a finite c, such that $|f(x)| \leqq c$, except perhaps for a set of ψ-measure zero; thus we have

$$(Q_\nu - B)\int f d\psi = \theta_2 c\psi(Q_\nu - B), \qquad |\theta_2| \leqq 1. \tag{5}$$

As f is approximately continuous at a, we have $d(a, B, \psi, \mathfrak{Q}) = 1$, thus $\psi(Q_\nu B)/\psi(Q_\nu) \to 1$, and therefore

[17] J. Radon, Sitzungsberichte, Akademie der Wissenschaften, Vienna, IIa, vol. 122 (1913), pp. 1324–1332; M. Fréchet, Comptes Rendus de l'Académie des Sciences, Paris, vol. 160 (1915), pp. 839–840; Bulletin de la Société Mathématique de France, vol. 43 (1915), pp. 248–265.

[18] That the condition, f be ψ-bounded, is essential is already shown by an example given by A. Denjoy, loc. cit., p. 173 (for the 1-dimensional case and ψ meaning Lebesgue's linear measure).

$$\frac{\psi(Q_\nu - B)}{\psi(Q_\nu)} \to 0. \tag{6}$$

As $\epsilon > 0$ is arbitrarily small, both these relations, together with (3), (4), (5) give $\phi(Q_\nu)/\psi(Q_\nu) \to f(a)$.

THEOREM 2. *In Theorem* 1, *the derivative* $D(a, \phi, \psi, \mathfrak{Q})$ *is regular.*

PROOF. Let $((M_\nu))$ be a sequence of sets regularly converging to a (for ψ relative to $\mathfrak{Q}$); that is, there must exist a sequence $Q_\nu \in \mathfrak{Q}_a$ converging to a, and a $\zeta > 0$, such that (1) hold. Because of Lemma 4, we can assume: $\psi(Q_\nu) \neq 0$, thus according to (1) also $\psi(M_\nu) \neq 0$. Now (1), (6) imply: $\psi(M_\nu - B)/\psi(M_\nu) \to 0$, and therefore $\psi(M_\nu B)/\psi(M_\nu) \to 1$. As (3), (4), (5) hold, if we substitute M_ν for D_ν, we get as before: $\phi(M_\nu)/\psi(M_\nu) \to f(a)$.

An inverse of the Theorems 1 and 2 is contained in the following theorem, for which, however, we do not have to assume that f is ψ-bounded, but only that it is ψ-integrable.

THEOREM 3. *Let* $\mathfrak{Q}$ *be an indefinitely fine system and* $\phi(M) = (M)\int f d\psi$. *If at the point* $a \in R - R^*$, *the derivative* $D(a, \phi, \psi, \mathfrak{Q})$ *is regular and equal to* $f(a)$, *then* f *is approximately continuous at* a *(for* ψ *relative to* $\mathfrak{Q}$*).*

PROOF. Assume that f is not approximately continuous at a (for ψ relative to $\mathfrak{Q}$). Then, because of Lemma 6, there exists either a $y > f(a)$ or a $y' < f(a)$, such that the upper density (for ψ relative to $\mathfrak{Q}$) of the set $[f(x) \geqq y] = C$ or $[f(x) \leqq y'] = C'$ is positive at a. Suppose, we have the first case (the second case is to be treated in the same way). There exists a sequence of sets $Q_\nu \in \mathfrak{Q}_a$, converging to a, so that $\psi(C \cdot Q_\nu)/\psi(Q_\nu) \to \bar{d}(a, C, \psi, \mathfrak{Q}) > 0$; thus there exists a $\zeta(a) > 0$, so that $\psi(CQ_\nu) > \zeta(a) \cdot \psi(Q_\nu) > 0$ for almost all ν, that is, the sequence $((C \cdot Q_\nu))$ converges regularly to a (for ψ relative to $\mathfrak{Q}$). Because $f(x) \geqq y$ on C and $y > f(a)$, we therefore have $\phi(CQ_\nu) = (CQ_\nu)\int f d\psi \geqq y\psi(CQ_\nu) > f(a)\psi(CQ_\nu)$ for almost all ν; thus the sequence $\phi(CQ_\nu)/\psi(CQ_\nu)$ cannot converge to $f(a)$.

The Theorems 1, 2, 3, together give the following result:

THEOREM 4. *Let* $\mathfrak{Q}$ *be an indefinitely fine system, let* f *be* ψ*-measurable and* ψ*-bounded in* R, *and* $\phi(M) = (M)\int f d\psi$. *In order that at the point* $a \in R - R^*$, ϕ *have the regular derivative* $D(a, \phi, \psi, \mathfrak{Q}) = f(a)$, *it is necessary and sufficient, that* f *be approximately continuous at* a *for* ψ *relative to* $\mathfrak{Q}$.

UNIVERSITY OF NEW MEXICO

A NOTE ON HILBERT'S OPERATOR

H. KOBER

The transformation

$$(1)\quad \mathfrak{H}f = \frac{1}{\pi} P\,V \int_{-\infty}^{\infty} \frac{f(t)}{t-x}\,dt = \frac{1}{\pi} \lim_{\epsilon \to 0} \int_{\epsilon}^{\infty} \frac{dt}{t} \{f(x+t) - f(x-t)\}$$

is well known to have the following properties:

LEMMA 1.[1] *When $1<p<\infty$, then $\mathfrak{H}f$ is a continuous (bounded) linear transformation with both domain and range $L_p(-\infty, \infty)$, and $\mathfrak{H}^2 f = -f$.*

LEMMA 2.[2] *When $f(t)\in L_1(-\infty, \infty)$, then $\mathfrak{H}f$ exists for almost all x in $(-\infty, \infty)$, but does not necessarily belong to $L_1(a, b)$, where a, b are arbitrary numbers $(-\infty \leqq a < b \leqq \infty)$; however $(1+x^2)^{-1} |\mathfrak{H}f|^q \in L_1(-\infty, \infty)$ when $0<q<1$. When f and $\mathfrak{H}f$ belong to $L_1(-\infty, \infty)$, then $\mathfrak{H}^2 f = -f$.*

The case $p=1$ appears to present the greatest difficulties. In the present note I shall deal with the set of elements $f(t)\in L_1(-\infty, \infty)$ for which $\mathfrak{H}f \in L_1(-\infty, \infty)$. In consequence of the lemmas, in this set or in $L_p(-\infty, \infty)$ $(1<p<\infty)$, $\mathfrak{H}f$ has no characteristic values other than $\pm i$. We shall start from the sets of characteristic functions and, incidentally, from the class $\mathfrak{H}_p$, the theory of which has been developed by E. Hille and J. D. Tamarkin; $\mathfrak{H}_p$ is the set of functions $F(z)$ $(z=x+iy)$ which, for $y>0$, are regular and satisfy the inequality

$$(2)\qquad \int_{-\infty}^{\infty} |F(x+iy)|^p dx \leqq M^p \quad \text{or} \quad |F(z)| \leqq M$$

for $0<p<\infty$ or $p=\infty$, respectively, where M depends on F and p only.[3] By $\mathfrak{K}_p$ we denote the corresponding class defined for $y<0$, and by $F(t)$, $G(t)$ the limit-functions[3] $(y\to 0;\ x=t)$ of elements $F(z)\in\mathfrak{H}_p$, $G(z)\in\mathfrak{K}_p$. By $\mathfrak{H}_p'$ and $\mathfrak{K}_p'$, respectively, we denote the two sets of those limit-functions, and by $\mathfrak{H}_p' \dotplus \mathfrak{K}_p'$ the smallest linear manifold

---

Received by the editors August 5, 1941.

[1] M. Riesz, Mathematische Zeitschrift, vol. 27 (1928), pp. 218–244.

[2] E. C. Titchmarsh, *Introduction to the Theory of Fourier Integrals*, Oxford, 1937, §5.14. E. Hille and J. D. Tamarkin, Fundamenta Mathematicae, vol. 25 (1935), pp. 329–352. Comparing our notation with that of Hille-Tamarkin, we have $\mathfrak{H}f = -\tilde{f}$.

[3] Loc. cit., $1 \leqq p < \infty$. T. Kawata, Japanese Journal of Mathematics, vol. 13 (1936), pp. 421–430, $0<p<\infty$. The limit-functions exist for almost all t in $(-\infty, \infty)$ and belong to $L_p(-\infty, \infty)$.

containing both $\mathfrak{H}_p'$ and $\mathfrak{K}_p'$. Obviously an element $f(t)$ belongs to $\mathfrak{H}_p' \dotplus \mathfrak{K}_p'$ if and only if it can be represented in the form

$$(3) \qquad f(t) = F(t) + G(t) = F(t) + \overline{F}_1(t), \quad F \in \mathfrak{H}_p', F_1 \in \mathfrak{H}_p', G \in \mathfrak{K}_p',$$

and this representation is unique, except for a constant when $p = \infty$.

Theorem 1 (b), as yet unpublished, is due to H. R. Pitt, Aberdeen, to whom I am greatly indebted.

We obtain the following results:

LEMMA 3. *Let $1 \leqq p \leqq \infty$; let the norm of an element $\phi(z)$ belonging to $\mathfrak{H}_p$ or $\mathfrak{K}_p$ be defined by*

$$(4) \qquad |\phi(t)|_p = \left\{ \int_{-\infty}^{\infty} |\phi(t)|^p dt \right\}^{1/p} \quad \text{or} \quad |\phi(t)|_p = \operatorname*{ess.u.b.}_{-\infty<t<\infty} |\phi(t)|$$

for $1 \leqq p < \infty$ or $p = \infty$, respectively. Then $\mathfrak{H}_p$ and $\mathfrak{K}_p$ are complete normed linear spaces, that is to say, (B) spaces in the terminology of Banach.

THEOREM 1. *Let $f(t) \in L_1(-\infty, \infty)$.* (a) *A necessary condition that $\mathfrak{H}f \in L_1(-\infty, \infty)$ is*

$$(5) \qquad \int_{-\infty}^{\infty} f(t)dt = 0.$$

(b) *(Pitt's theorem.) The condition is not sufficient.*

THEOREM 2. (a) *A necessary and sufficient condition that both f and $\mathfrak{H}f$ belong to $L_1(-\infty, \infty)$ is that f belongs to $\mathfrak{H}_1' \dotplus \mathfrak{K}_1'$.* (b) *With domain $\mathfrak{H}_1' \dotplus \mathfrak{K}_1'$, $\mathfrak{H}f$ is a linear closed[4] unbounded transformation in $L_1(-\infty, \infty)$.*

THEOREM 3. *The set $\mathfrak{H}_1' \dotplus \mathfrak{K}_1'$ is a non-closed subspace of L_1 and is nowhere dense in L_1. Its closure is the subset of L_1 satisfying* (5).

We note that, by Lemma 1 and by the argument which will be employed in the proof of Theorem 2(a), $\mathfrak{H}_p' \dotplus \mathfrak{K}_p' = L_p$ for $1 < p < \infty$.

We shall now give the proofs of the above results; some examples will be given at the end of this paper.

Proof of Lemma 3. We need only show that the space $\mathfrak{H}_p$ is complete. Let $\{F_n(z)\} \in \mathfrak{H}_p$, $n = 1, 2, \cdots$, be a sequence satisfying the condition of convergence $|F_n(t) - F_m(t)|_p \to 0$ $(m > n \to \infty)$. Then there exists an element $F(t) \in L_p$ such that $|F(t) - F_n(t)|_p \to 0$ as $n \to \infty$; we have to show that $F(t)$ is the limit-function of an element $\varphi(z) \in \mathfrak{H}_p$.

[4] That is to say, $f_n \in \mathfrak{H}_1' \dotplus \mathfrak{K}_1'$, $g_n = \mathfrak{H}f_n$ $(n = 1, 2, \cdots)$, $|f - f_n|_1 \to 0$ and $|g - g_n|_1 \to 0$ imply $g = \mathfrak{H}f$.

By a result due to Hille and Tamarkin,[5] $F_n(z)$ is represented by its "proper Poisson integral"

$$(6)\qquad F_n(z) = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{yF_n(t)dt}{(t-x)^2+y^2} = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{yF_n(t+x)}{t^2+y^2}\,dt,$$

$$z = x + iy;\ y \to 0.$$

Let

$$(7)\qquad \varphi(z) = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{yF(t+x)}{t^2+y^2}\,dt.$$

For $y \geqq \epsilon > 0$, by Hölder's theorem, we have uniformly

$$(8)\qquad |\varphi(z) - F_n(z)| \leqq \pi^{-1}\epsilon^{-1/p}\,|(t^2+1)^{-1}|_{p'}\,|F(t) - F_n(t)|_p \to 0$$

as $n \to \infty$, where $1/p + 1/p' = 1$. Hence $\varphi(z)$ is a regular function fo $y > 0$, and it is obviously bounded when $p = \infty$.

Now let $1 \leqq p < \infty$. By a well known convexity theorem,

$$(9)\qquad \begin{aligned}\int_{-\infty}^{\infty} |\varphi(x+iy)|^p dx &\leqq \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{ydt}{t^2+y^2}\int_{-\infty}^{\infty} |F(t+x)|^p dx \\ &= \int_{-\infty}^{\infty} |F(x)|^p dx.\end{aligned}$$

Thus $\varphi(z) \in \mathfrak{H}_p$. By the same argument and by Fatou's theorem,

$$\begin{aligned}|\varphi(t) - F_n(t)|_p &\leqq \liminf_{y \to 0}\left\{\int_{-\infty}^{\infty} |\varphi(z) - F_n(z)|^p dx\right\}^{1/p} \\ &\leqq |F(t) - F_n(t)|_p \to 0.\end{aligned}$$

By (8), the result holds for $p = \infty$. Therefore $F(t) \equiv \varphi(t)$, which completes the proof.

To prove Theorem 2(a) we require a result which we deduce from theorems by Hille and Tamarkin:

LEMMA 4. *A necessary and sufficient condition that $f(t)$ belongs to $L_p(-\infty, \infty)$ $(1 \leqq p < \infty)$ and that $\mathfrak{H}f = if$ or $\mathfrak{H}f = -if$ is that $f(t)$ belongs to $\mathfrak{H}_p'$ or $\mathfrak{K}_p'$, respectively.*

Let $f(t) \in \mathfrak{H}_p'$ and $f(t) = \varphi(t) + i\psi(t)$. Since $f(t)$ is the limit-function $(y \to 0, x = t)$ of an element $F(z) \in \mathfrak{H}_p$, and since $F(z)$ is represented by its proper Poisson integral, we have[6] $\psi(x) = -\mathfrak{H}\varphi$ and, by Lemmas 1

[5] Loc. cit., Theorem 2.1 (ii), $1 \leqq p < \infty$. The result holds for $p = \infty$.

[6] Hille and Tamarkin, loc. cit., Theorem 3.1. For $p = 2$, the lemma is an easy consequence of Theorem 95, Titchmarsh, loc. cit.

and 2, $\varphi(x)=\mathfrak{H}\psi$; therefore $\mathfrak{H}f=\mathfrak{H}(\varphi+i\psi)=-\psi+i\varphi=if$. Conversely, let $f(t)\in L_p$ and $\mathfrak{H}f=if$. For $y>0$, the function

$$F(z)=\frac{1}{2\pi i}\int_{-\infty}^{\infty}\frac{f(t)}{t-z}\,dt$$

is regular and representable by its proper Poisson integral, and its limit function is $(1/2)\{f(x)-i\mathfrak{H}f\}=(1/2)(f(x)+f(x))=f(x)$.[6] Hence $F(z)\in\mathfrak{H}_p$, and so $f(t)\in\mathfrak{H}_p'$, which proves the lemma.

Proof of Theorem 2(a). Let $f\in L_1$ and $\mathfrak{H}f\in L_1$, then the functions

$$F=(1/2)(f-i\mathfrak{H}f),\qquad G=(1/2)(f+i\mathfrak{H}f)$$

belong to L_1; by Lemma 2, $\mathfrak{H}^2f=-f$, and so $\mathfrak{H}F=iF$, $\mathfrak{H}G=-iG$. By Lemma 4, we have $F\in\mathfrak{H}_1'$, $G\in\mathfrak{K}_1'$, and so $f=F+G\in\mathfrak{H}_1'+\mathfrak{K}_1'$.

Conversely, let $f\in\mathfrak{H}_1'+\mathfrak{K}_1'$. Then, by (3) with $p=1$, and by Lemma 4,

$$\mathfrak{H}f=\mathfrak{H}F+\mathfrak{H}G=i(F-G)\in L_1(-\infty,\infty),$$

which proves Theorem 2(a). Part (b) will be proved after Theorem 3.

To prove Theorem 1, we need a further result due to Hille and Tamarkin.[7]

LEMMA 5. *Let $1\leqq p<\infty$, Let $\phi(t)$ belong to L_p and possess a Fourier transform $\psi(x)$,*

$$\psi(x)=(2\pi)^{-1/2}\operatorname*{l.i.m.}_{N\to\infty}\text{ index }p'\int_{-N}^{N}\phi(t)e^{-itz}dt,\qquad 1/p+1/p'=1.$$

Then $\phi(t)\in\mathfrak{H}_p'$ or $\mathfrak{K}_p'$ if and only if $\psi(x)$ vanishes in $(-\infty,0)$ or in $(0,\infty)$, respectively.

For completeness we add the following result:

LEMMA 5′. *Let $2<p<\infty$ and let $\phi(t)$ belong to L_p and have no Fourier transform in $L_{p'}$. Then $\phi(t)\in\mathfrak{H}_p'$ or $\mathfrak{K}_p'$ if and only if there is a sequence $\{\phi_n(t)\}$ belonging to $\mathfrak{H}_p'$ or $\mathfrak{K}_p'$ and satisfying the hypotheses of Lemma 5 and such that $|\phi(t)-\phi_n(t)|_p\to 0$ as $n\to\infty$.*[8]

[7] Loc. cit., Lemma 4.2, and Annals of Mathematics, (2), vol. 34 (1933), pp. 606–614, Theorem 3.

[8] The proof is similar to that given for the generalization of a theorem due to Paley-Wiener; H. Kober, Quarterly Journal of Mathematics, vol. 11 (1940), pp. 66–80, Theorem 2(b). Let $\phi(t)\in\mathfrak{H}_p'$ and $|\phi(t)-f_n(t)|_p\to 0$, where $f_n(t)$ $(n=1,2,\cdots)$ has a Fourier transform in $L_{p'}$; then the functions $\phi_n(t)=(1/2)(f_n-i\mathfrak{H}f_n)$ have the desired properties. The converse is proved by Lemma 3.

By Theorem 2 and Lemma 5, $f(t)$ can be represented as the sum of two functions $F(t)$, $G(t)$ belonging to L_1 and such that their Fourier transforms $\varphi(x)$, $\psi(x)$ vanish for $x<0$ or $x>0$, respectively. By continuity, they also vanish at $x=0$; so does the Fourier transform of $f(t)$, which gives (5). For the Fourier transform of an element $F(t)\in L_1$ is continuous in $(-\infty, \infty)$.

To prove Theorem 1(b), take $f_1(t)=t^{-1}\log^{-2} t$ and $f_2=2/\log 2$ in $(0, 1/2)$, $f_1(t)=f_2(t)=0$ otherwise. Let $f(t)=f_1(t)-f_2(t)$, then obviously $f(t)$ belongs to $L_1(-\infty, \infty)$ and satisfies (5). But $\mathfrak{H}f$ does not belong to $L_1(-\infty, \infty)$, since

$$\int_{-1/2}^{0} |\mathfrak{H}f_1|\,dx = \infty,$$

$$\int_{-1/2}^{0} |\mathfrak{H}f_2|\,dx = \frac{2}{\pi \log 2}\int_{-1/2}^{0} \left|\log\left|1-\frac{1}{2x}\right|\right| dx < \infty.$$

For, in $(0, 1/2)$, we have

$$\mathfrak{H}[f_1; -x] = \frac{1}{\pi}\int_0^{1/2} \frac{\log^{-2} t\,dt}{(x+t)t} \geqq \frac{1}{\pi}\int_0^{x} \frac{\log^{-2} t\,dt}{(x+t)t}$$

$$\geqq \frac{1}{\pi}\int_0^{x} \frac{\log^{-2} t\,dt}{2xt} = \frac{1}{2\pi x|\log x|};$$

hence $\mathfrak{H}f_1$ does not belong to $L_1(-1/2, 0)$, which proves the theorem.

Proof of Theorem 3. Let E be the subset of L_1 satisfying (5). By Theorems 1 and 2, $\mathfrak{H}_1' + \mathfrak{K}_1'$ is a subset of E and different from E. It is easy to see that E is closed in L_1. We are left to show that E is the closure of $\mathfrak{H}_1' + \mathfrak{K}_1'$.

Let $f(t)$ be a step-function belonging to E. Denoting by $\epsilon(t)$ the step-function which is equal to 1 in $(0, 1)$ and to zero otherwise, we can represent $f(t)$ by a finite sum $\sum a_n \epsilon(t/b_n)$ ($b_n \lessgtr 0$, a_n complex). By (5), $\sum a_n |b_n| = 0$, and so

$$\pi\mathfrak{H}f = \sum a_n\left(\log\left|1-\frac{b_n}{x}\right|\right)\operatorname{sgn} b_n = O(x^{-2}), \qquad x \to \pm\infty.$$

Hence $\mathfrak{H}f \in L_1$, $f \in \mathfrak{H}_1' + \mathfrak{K}_1'$. We can now approximate to any $f(t)\in E$ by a sequence $\{f_n(t)\}$ ($n=1, 2, \cdots$) of step-functions belonging to $\mathfrak{H}_1' + \mathfrak{K}_1'$. Let $f(t)$ satisfy (5), and let $\{g_n(t)\}$ be a sequence of step-functions such that $|f(t)-g_n(t)|_1 \to 0$ as $n\to\infty$. Take

$$f_n(t) = g_n(t) - \epsilon(t)\int_{-\infty}^{\infty} g_n(\xi)\,d\xi, \qquad n = 1, 2, \cdots.$$

Then $f_n(t)$ is a step-function, $f_n(t)$ satisfies (5); therefore $f_n \in \mathfrak{H}_1' + \mathfrak{K}_1'$. Finally, by (5), we have

$$|f - f_n|_1 = \left| f - g_n - \epsilon \int_{-\infty}^{\infty} \{f(\xi) - g_n(\xi)\} d\xi \right|_1$$

$$\leqq |f - g_n|_1 + \left| \int_{-\infty}^{\infty} \{f(\xi) - g_n(\xi)\} d\xi \right| \leqq 2|f - g_n|_1,$$

which tends to zero as $n \to \infty$. Thus E is the closure of $\mathfrak{H}_1' + \mathfrak{K}_1'$.

The set E is nowhere dense in L_1. For when $f \in L_1$, then, given $\epsilon > 0$, any element $g(t) = f(t) + \delta\epsilon(t)$ $(0 < |\delta| < \epsilon)$ belongs to the sphere $|g - f|_1 < \epsilon$, while g does not belong to E; when f belongs to L_1 but not to E, then no element g of the sphere $|g - f|_1 < |\int f(t)dt|$ belongs to E. Thus we have proved the theorem.

Proof of Theorem 2(b). In the domain $\mathfrak{H}_1' + \mathfrak{K}_1'$, by Lemma 2, we have $i\mathfrak{H}(i\mathfrak{H}f) = f$; hence $i\mathfrak{H}f$ is involutory. By Lemma 3, both $\mathfrak{H}_1'$ and $\mathfrak{K}_1'$ are closed spaces in L_1. Therefore $i\mathfrak{H}f$, and therefore $\mathfrak{H}f$, is closed; for a linear involutory transformation in a (B) space is closed if and only if the spaces of the characteristic functions are closed.[9] By Theorem 3, $\mathfrak{H}_1' + \mathfrak{K}_1'$ is not closed. Therefore $\mathfrak{H}f$ is not bounded in this domain; for a linear closed transformation in a (B) space is continuous if and only if its domain is closed.[10] Thus we have proved the theorem.

The following are examples for the case $f \in L_1(-\infty, \infty)$, $\mathfrak{H}f \in L_1(-\infty, \infty)$. We may start from Lemma 4,[11] but it is easier to make use of Theorem 2.

(1) Let $T_1(z)$ or $T_2(z)$ be polynomials of degree $\alpha > 0$ or $\beta > 0$ and such that they have no zeros for $y \geqq 0$ or $y \leqq 0$, respectively; let a, b be any numbers such that $-\infty < a < -1/\alpha$, $-\infty < b < -1/\beta$. Then, on a suitable Riemann surface, any branch of $\{T_1(z)\}^a$ $(y > 0)$ or $\{T_2(z)\}^b$ $(y < 0)$ belongs to $\mathfrak{H}_1$ or $\mathfrak{K}_1$, respectively. When $f(t) = \{T_1(t)\}^a + \{T_2(t)\}^b$, by Lemma 4, we have $\mathfrak{H}f = i\{T_1(x)\}^a - i\{T_2(x)\}^b \in L_1$.

(2) Let $\varphi_1(z) = (1 - \cos \alpha z)z^{-2}$, $\varphi_2(z) = \{\sin \alpha z - 2\sin(\alpha z/2)\}z^{-2}$, $\alpha > 0$, and let $f(t) = A\varphi_1(t)e^{i\alpha t} + B\varphi_2(t)e^{-i\alpha t}$; then $\mathfrak{H}f = iA\varphi_1(x)e^{i\alpha x} - iB\varphi_2(x)^{-i\alpha x}$, and $f \in L_1$, $\mathfrak{H}f \in L_1$. It can be shown that this result holds when $\varphi_j(z)$ $(j = 1, 2)$ are integral functions such that $\varphi_j(t) \in L_1$ and that, for any $\epsilon > 0$, $|\varphi_j(z)| < K_\epsilon \exp\{(\alpha + \epsilon)|z|\}$; in this way we can construct

[9] H. Kober, Proceedings of the London Mathematical Society, (2), vol. 44 (1938), pp. 453–465, Theorem 6′(a).

[10] S. Banach, *Théorie des Opérations Linéaires*, Warsaw, 1932, p. 41, Theorem 7. Probably the converse is well known.

[11] Or from Theorem 3.1, Hille and Tamarkin, loc. cit.

all integral functions $f(z)$ satisfying the conditions $f(t)\in L_1$, $\mathfrak{F}f\in L_1$, $|f(z)|<K_{f,\epsilon}\exp\{(2\alpha+\epsilon)|z|\}$. The proof is based upon a result due to Plancherel and Pólya.[12]

THE UNIVERSITY,
EDGBASTON, BIRMINGHAM, ENGLAND

[12] Commentarii Mathematici Helvetici, vol. 10 (1937–1938), pp. 110–163, §27.

THE BEHAVIOR OF CERTAIN STIELTJES CONTINUED FRACTIONS NEAR THE SINGULAR LINE

H. S. WALL

1. **Introduction.** We consider here continued fractions of the form[1]

$$(1.1)\qquad f(z)=\frac{g_0}{1+}\,\frac{g_1z}{1+}\,\frac{(1-g_1)g_2z}{1+}\,\frac{(1-g_2)g_3z}{1+}\cdots,$$

in which $g_0\geqq 0$, $0\leqq g_n\leqq 1$, $(n=1, 2, 3, \cdots)$, it being agreed that the continued fraction shall terminate in case some partial numerator vanishes identically. There exists a monotone non-decreasing function $\phi(u)$, $0\leqq u\leqq 1$, such that

$$(1.2)\qquad f(z)=\int_0^1\frac{d\phi(u)}{1+zu};$$

and, conversely, every integral of this form is representable by such a continued fraction. Put $M(f)=\text{l.u.b.}_{|z|<1}|f(z)|$. Then $M(f)\leqq 1$ if and only if the continued fraction can be written in the form

$$(1.3)\qquad f(z)=\frac{h_1}{1+}\,\frac{(1-h_1)h_2z}{1+}\,\frac{(1-h_2)h_3z}{1+}\cdots,$$

in which $0\leqq h_n\leqq 1$, $(n=1, 2, 3, \cdots)$. These functions are analytic in the interior of the z-plane cut along the real axis from $z=-1$ to $z=-\infty$.

The principal object of this paper is to prove the following theorem:

THEOREM 1.1. *If* $0<h_n<1$, $(n=1, 2, 3, \cdots)$, *and* $h_n\to 1/2$ *in such a way that the series* $\sum|h_n-1/2|$ *converges, then the function* $f(z)$ *given*

Presented to the Society, October 25, 1941; received by the editors August 14, 1941.

[1] H. S. Wall, *Continued fractions and totally monotone sequences*, Transactions of this Society, vol. 48 (1940), pp. 165–184.

by (1.3) *approaches a finite limit* $\alpha(s)$ *as* $z\to -s$, $s\geqq 1$, *from the upper half-plane, and the limit* $\overline{\alpha(s)}$, *the complex conjugate of* $\alpha(s)$, *as* $z\to -s$ *from the lower half-plane. The function* $\alpha(s)$ *is continuous, and is real if and only if* $s=1$. *There is a constant* C *such that* $|f(z)|<C$ *over the entire plane of* z *exterior to the cut along the real axis from* $z=-1$ *to* $z=-\infty$.

Inasmuch as the function (1.1) can be written in the form $f(z)=g_0/[1+zf^*(z)]$, where $f^*(z)$ has the form (1.3), one may conclude at once that if $g_0>0$, $0<g_n<1$, $(n=1, 2, 3, \cdots)$, $\sum|g_n-1/2|$ converges, then the function $f(z)$ given by (1.1) approaches a finite limit $\beta(s)$ as $z\to -s$, $s>1$, from the upper half-plane, and the limit $\overline{\beta(s)}$ as $z\to -s$ from the lower half-plane. The function $\beta(s)$ is continuous and not real for $s>1$. The function $f(z)$ given by (1.1) may become infinite as $z\to -1$, for example, if $g_0=1$, $g_n=1/2$ $(n=1, 2, 3, \cdots)$, then $f(z)=(1+z)^{-1/2}$.

2. **Proof of Theorem** 1.1. There is a one to one correspondence between functions of the form (1.3) and functions $e(x)$ which are real when x is real, analytic for $|x|<1$, and for which $M(e)\leqq 1$, such that if $f(z)\leftrightarrow e(x)$ then[2]

$$(2.1)\qquad \frac{1}{2}(1-x)\frac{1-e(x)}{1+xe(x)}=f(z),\quad z=4x/(1-x)^2,\quad |x|<1.$$

(i) The transformation $z=4x/(1-x)^2$ maps the interior of the circle $|x|=1$ one to one upon the interior of the z-plane cut along the real axis from $z=-1$ to $z=-\infty$. Hence it follows at once from (2.1) that if $M(e)<1$, then

$$|f(z)|\leqq\frac{1+M(e)}{1-M(e)}=C,$$

over the entire domain of analyticity of $f(z)$.

(ii) In (2.1) put $x=\xi+i\eta$, $e(x)=u+iv$, $f(z)=P+iQ$, where ξ, η, u, v, P, Q are all real. We then find for Q the value

$$(2.2)\qquad Q=\frac{\eta(u^2+v^2-1)+v(\xi^2+\eta^2-1)}{2|1+xe(x)|^2}.$$

If $s\geqq 1$, $\sigma=[s-2+2i(s-1)^{1/2}]/s$, so that $|\sigma|=1$, then as $x\to\sigma$ from the interior of the circle $|x|=1$, z must approach $-s$ from the upper half-plane. If $M(e)<1$, and $e(x)$ approaches a limit $e(\sigma)$ as $x\to\sigma$, $|x|<1$, then it follows from (2.1) that $f(z)$ approaches a finite limit

[2] H. S. Wall, *Some recent developments in the theory of continued fractions*, this Bulletin, vol. 47 (1941), pp. 405–423; Theorem 5.1, p. 415.

$\alpha(s)$ as $z \to -s$ from the upper half-plane; and from (2.2) it follows that Q has the limit

$$\frac{(s-1)^{1/2}}{s} \cdot \frac{|e(\sigma)|^2 - 1}{|1+\sigma e(\sigma)|^2}, \tag{2.3}$$

where is zero if and only if $s=1$. Hence $\alpha(s)$ is real if and only if $s=1$. Inasmuch as $f(\bar{z}) = \overline{f(z)}$, it follows that $f(z)$ has the limit $\overline{\alpha(s)}$ as $z \to -s$ from the lower half-plane. Clearly $\alpha(s)$ is continuous if $e(x)$ is continuous for $|x| \leqq 1$.

(iii) To complete the proof of Theorem 1.1 it remains to be proved that when $\sum |h_n - 1/2|$ converges then $M(e) < 1$ and $e(x)$ is continuous for $|x| \leqq 1$. Put $e_0(x) = e(x)$,

$$e_{n+1}(x) = \frac{1}{x} \frac{t_n - e_n(x)}{1 - t_n e_n(x)}, \qquad t_n = e_n(0);\ n = 0, 1, 2, \cdots. \tag{2.4}$$

Then $t_{n-1} = 1 - 2h_n$ $(n = 1, 2, 3, \cdots)$. Now, Schur[3] proved that if $|t_{n-1}| < 1$, $(n = 1, 2, 3, \cdots)$, and $\sum |t_n|$ is convergent, then $M(e) < 1$, and $e(x)$ is continuous for $|x| \leqq 1$. Since $0 < h_n < 1$ by hypothesis, it follows that $-1 < t_{n-1} < 1$; and since the series $\sum |h_n - 1/2|$ converges by hypothesis, it follows that $\sum |t_n|$ converges.

This completes the proof of Theorem 1.1.

It will be seen from (2.3) that if $f(z)$ has a real limit as $z \to -s$, $s > 1$, then $M(e) = 1$. This is true also if $f(z)$ becomes infinite as $z \to -s$, $s \geqq 1$, and in this case $e(x) \to -1/\sigma$ as $x \to \sigma$. Inasmuch as $\lim_{z \to -s} (z+s) f(z) = 0$, $\lim_{z \to \infty} f(z) = 0$, if $M(e) < 1$, it follows that the corresponding mass function $\phi(u)$ (cf. (1.2)), is continuous for $0 \leqq u \leqq 1$ in this case.[4]

3. **An example.** If we apply the transformation (2.4) to a function $f(z)$ of the form (1.3) we obtain a sequence of functions $f_0(z) = f(z)$, $f_1(z)$, $f_2(z)$, $\cdots$ all having continued fraction expansions of the same character as that of $f(z)$. Suppose that in (1.3), $0 < h_n < 1$, $(n = 1, 2, 3, \cdots)$, and that the series $\sum |h_n - 1/2|$ converges. On applying Theorem 1.1 we find at once that as $z \to -s$, $s \geqq 1$, $I(z) > 0$:

$$\lim f_1(z) = -\frac{1}{s} \frac{g_1 - \alpha(s)}{1 - g_1 \alpha(s)} = \alpha_1(s);$$

and that $\alpha_1(s)$ is real if and only if $s = 1$; $\alpha_1(1) = 1$; $\alpha_1(s)$ is continuous for $s \geqq 1$. By mathematical induction, $f_2(z)$, $f_3(z)$, $\cdots$ also have this

[3] I. Schur, *Über Potenzreihen, die im Innern des Einheitskrieses beschränkt sind*, Journal für die reine und angewandte Mathematik, vol. 147 (1916), pp. 205–232, and vol. 148 (1917), pp. 122–145.

[4] I. J. Schoenberg, *Über die asymptotische Verteilung reeller Zahlen* mod 1, Mathematische Zeitschrift, vol. 28 (1928), pp. 171–199; p. 179.

property. Let $h_1'/1+(1-h_1')h_2'z/1+(1-h_2')h_3'z/1+\cdots$ be the continued fraction for $f_1(z)$. *Then we shall prove that* $\sum|h_n'-1/2|$ *may diverge although* $\sum|h_n-1/2|$ *converges, and that the convergence of the series* $\sum|h_n-1/2|$ *is not necessary in order that the conclusion in Theorem* 1.1 *shall hold.* For this purpose, let $h_n=1/2$, $(n=1, 2, 3, \cdots)$. Then $f(z)=1/[1+(1+z)^{1/2}]$, $(f(0)=1/2)$, and $f_1(z)=1/[1+(1+z)^{1/2}][1+2(1+z)^{1/2}]$, $(f_1(0)=1/6)$. The function $f_1(z)$ has the properties stated in Theorem 1.1 for the function $f(z)$ of that theorem, excepting that, as we shall see, the series $\sum|h_n'-1/2|$ diverges. In fact, $h_{2n}'=(4n+3)/2(4n+1)$, $h_{2n-1}'=(4n-3)/2(4n-1)$, $(n=1, 2, 3, \cdots)$, in consequence of the following theorem:

THEOREM 3.1. *Let* k *be a parameter subject only to the conditions*

$$k \neq (3-4n)/2, \quad (1-4n)/2, \qquad n = 1, 2, 3, \cdots, \tag{3.1}$$

and put

$$h_{2n-1}^{(k)} = (4n-3)/2(4n-3+2k),$$
$$h_{2n}^{(k)} = (4n-1+4k)/2(4n-1+2k), \qquad n = 1, 2, 3, \cdots.$$

Then the continued fraction $f_k(z)=h_1^{(k)}/1+(1-h_1^{(k)})h_2^{(k)}z/1+(1-h_2^{(k)})h_3^{(k)}z/1+\cdots$ *converges uniformly in a sufficiently small neighborhood of* $z=0$, *and the analytic function* $f_k(z)$ *satisfies the relation*

$$f_{k+1}(z) = \frac{1}{z}\,\frac{h_1^{(k)} - f_k(z)}{1 - h_1^{(k)} f_k(z)}. \tag{3.2}$$

PROOF. The uniform convergence follows from the fact that all the partial numerators after the first are numerically less than or equal to $1/4$ for z in a sufficiently small neighborhood of the origin. To prove (3.2), write the right-hand member in the form:

$$\frac{1}{z}\left\{h_1^{(k)} - \frac{1-(h_1^{(k)})^2}{-h_1^{(k)}+1/f_k(z)}\right\} = \frac{1}{z}\left\{h_1^{(k)} - \frac{h_1^{(k)}}{1} + \frac{h_2^{(k)}z/(1+h_1^{(k)})}{1} + \frac{(1-h_2^{(k)})h_3^{(k)}z}{1} + \frac{(1-h_3^{(k)})h_4^{(k)}z}{1} + \cdots\right\}.$$

We are to show that this is equal to $f_{k+1}(z)$. This can be done by showing that the odd part of the last continued fraction is identical with

the even part of the continued fraction for $f_{k+1}(z)$. We omit here the details of the calculation.[5]

Let $e_n(x) \leftrightarrow f_n(z)$, $(n=0, 1, 2, \cdots)$. Then we find for the e_n's the following recursion formulas:

$$(3.3) \qquad e_{n+1}(x) = \frac{1}{x} \frac{k_n + (2-k_n)x + (3x-1)e_n(x)}{(3-x) + (2-k_n+k_nx)e_n(x)}, \quad k_n = e_n(0),$$

$(n=0, 1, 2, \cdots)$. For the special example under consideration, $e(x)=e_0(x)\equiv 0$ and $e_1(x)=2/(3-x)$. Hence, although $M(e)<1$ in this case, nevertheless $M(e_1)=1$. From the way in which (3.3) was obtained it follows that if $e_0(x)$ is an arbitrary function which is real when x is real, analytic for $|x|<1$, and such that $M(e_0)\leqq 1$, then the functions $e_1(x)$, $e_2(x)$, $\cdots$ are all of this same character.

NORTHWESTERN UNIVERSITY

[5] O. Perron, *Die Lehre von den Kettenbrüchen*, 2d edition, Leipzig and Berlin, 1929, p. 201.

ON LOCAL CONVEXITY IN HILBERT SPACE

I. J. SCHOENBERG

1. **Introduction.** Let M be a set of points in a normed vector space V. M is said to be convex if p and q being any two points of M, the whole rectilinear segment $\overline{pq}$ belongs to M. A weakened form of convexity, due to H. Tietze,[1] is as follows:

DEFINITION OF LOCAL CONVEXITY. *Let $p \in M$. The set M is said to be locally convex at p if there exists a positive $\rho = \rho(p)$ such that the intersection $M \cdot S(p; \rho)$, of M with the open sphere $S(p; \rho)$ of center p and radius ρ, is convex in the ordinary sense. The set M is called locally convex if M is locally convex at all its points.*

Every convex set is locally convex. The converse is not true since every open set is obviously locally convex. Tietze's chief result concerning local convexity is as follows:

THEOREM 1 (of Tietze). *Let E_k denote the k-dimensional euclidean space. A closed and connected set M in E_k which is locally convex is also convex in the ordinary sense.*

By means of his concept of local euclidean dimension of a set M at a point $p \in M$, Tietze reduces the proof of Theorem 1 to the case of locally convex continua with interior points and which coincide with the closure of their set of interior points. Tietze then proves the theorem for continua in E_2 and finally extends the proof to cover any E_k. Tietze's method does not seem to be applicable for sets in Hilbert space.

The following lines contain a simpler method of dealing with this problem which allows the establishment of Tietze's theorem in any real or complex normed vector space whether separable or not. For the sake of definiteness we state and prove our theorem for real Hilbert space.[2]

Presented to the Society, September 8, 1939 under the title *On local convexity in euclidean spaces*; received by the editors August 13, 1941. The present note is an improved version (see Footnote 6).

[1] H. Tietze, *Über Konvexheit im kleinen und im grossen und über gewisse den Punkten einer Menge zugeordneten Dimensionszahlen*, Mathematische Zeitschrift, vol. 28 (1928), pp. 697–707.

[2] Recent results have demonstrated the breakdown of some classical properties of convex sets when we pass from euclidean spaces to Hilbert spaces. See, for example, David Moskowitz and L. L. Dines, *Convexity in linear spaces with an inner product*, Duke Mathematical Journal, vol. 5 (1939), pp. 520–534, in particular the example on

THEOREM 2. *A closed and connected set M in the real Hilbert space H which is locally convex is also convex in the ordinary sense.*

2. **On δ-convexity and three lemmas.** All our sets are in Hilbert space unless otherwise stated. A strengthened form of local convexity is as follows:

DEFINITION OF δ-CONVEXITY.[3] *Let δ be a positive number. A set is said to be δ-convex if p and q being any two points of M, of distance $pq<\delta$, the whole segment $\overline{pq}$ belongs to M.*

It is clear that δ-convexity implies local convexity. The converse is not true. Thus the following two sequences of points on the x-axis (space E_1)

$$M_1: \quad \left\{\frac{1}{n}\right\}, \qquad n = 1, 2, \cdots,$$

$$M_2: \quad \left\{1+\frac{1}{2}+\cdots+\frac{1}{n}\right\}, \qquad n = 1, 2, \cdots,$$

are clearly locally convex but not δ-convex, no matter how small δ may be. Notice that M_1 is bounded but not closed and M_2 is closed but not bounded, hence none of these two sets is self-compact. For self-compact sets both types of convexity are equivalent, a fact which we now state.

LEMMA 1. *A self-compact set M which is locally convex is also δ-convex for some appropriate value of δ.*

Indeed, the contrary assumption to the effect that M is never δ-convex, no matter how small δ is, implies that for every integer n our set M contains a pair of points a_n, b_n with $a_nb_n<1/n$ and such that the segment $\overline{a_nb_n}$ does not wholly belong to M. Since M is self-compact we may assume $a_n\to p$, $b_n\to p$ and $p\in M$. But this clearly contradicts the local convexity of M at the limiting point p.

---

pp. 531–532. This makes it the more remarkable that Tietze's theorem does hold in Hilbert space.

[3] The δ-convexity is readily seen to be equivalent to *uniform* local convexity. By this we mean local convexity of a set in the sense of our first definition with a radius $\rho=\rho(p)>0$ which is independent of p.

A δ-convex set is a very special instance of a *metric space with elementary arcs* in the sense of Marston Morse, *The Calculus of Variations in the Large*, American Mathematical Society Colloquium Publications, vol. 18, New York, 1934, p. 298. See also J. H. C. Whitehead, *Convex regions in the geometry of paths*, Quarterly Journal of Mathematics, vol. 3 (1932), pp. 33–42.

Our principal tool will be the following elementary geometrical lemma in euclidean space:

LEMMA 2.[4] *Let $p_0, p_1, \cdots, p_n$ $(p_0 \neq p_n)$ be points in the euclidean space E_k. Let Π denote the open polygonal line joining successively the given points $p_0, p_1, \cdots, p_n$. Regarding E_k as a vector space we derive a new sequence of points by setting*

$$p'_{-1} = p_0, \qquad p'_0 = \tfrac{1}{2}(p_0 + p_1), \qquad p'_1 = \tfrac{1}{2}(p_1 + p_2), \cdots,$$
$$p'_{n-1} = \tfrac{1}{2}(p_{n-1} + p_n), \quad p'_n = p_n.$$

Repeating the same operation on the newly derived broken line $\Pi' = p'_{-1}p'_0 \cdots p'_n$, let

$$p''_{-2} = p'_{-1} = p_0, \qquad p''_{-1} = \tfrac{1}{2}(p'_{-1} + p'_0), \qquad p''_0 = \tfrac{1}{2}(p'_0 + p'_1), \cdots,$$
$$p''_{n-1} = \tfrac{1}{2}(p'_{n-1} + p'_n), \qquad p''_n = p'_n = p_n.$$

Repeating this operation indefinitely we obtain an infinite sequence of broken lines

$$\Pi^{(m)} = p^{(m)}_{-m} p^{(m)}_{-m+1} \cdots p^{(m)}_n, \qquad m = 1, 2, 3, \cdots,$$

all joining the points p_0 and p_n. Let N be an open set containing the closed segment $\overline{p_0 p_n}$. Then N will contain the whole broken line $\Pi^{(m)}$ for all sufficiently large values of m.

Since our proof will be independent of the dimension k we may without loss of generality assume that $k = 2$. Let $p_i^{(0)} = p_i$ and $\Pi^{(0)} = \Pi$. For convenience we now extend the definition of the points $p_i^{(m)}$ $(-m \leqq i \leqq n)$ for all integral values of i $(= 0, \pm 1, \pm 2, \cdots)$ by setting

$$(1) \qquad \begin{aligned} p_i^{(m)} &= p_{-m}^{(m)} = p_0 \quad \text{if} \quad i \leqq -m, \\ p_i^{(m)} &= p_n^{(m)} = p_n \quad \text{if} \quad i \geqq n. \end{aligned}$$

We then have without exception the relation

$$p_i^{(m)} = \tfrac{1}{2}(p_i^{(m-1)} + p_{i+1}^{(m-1)}), \qquad m = 1, 2, \cdots; \; i = 0, \pm 1, \pm 2, \cdots,$$

and therefore

$$(2) \qquad p_i^{(m)} = \frac{1}{2^m}\{p_i + C_{m,1}p_{i+1} + C_{m,2}p_{i+2} + \cdots + p_{i+m}\}.$$

[4] Lemma 2 was suggested by the related problem (Number 3547) proposed by Martin Rosenman, American Mathematical Monthly, vol. 39 (1932), p. 239, and by its elegant solution due to R. E. Huston, ibid., vol. 40 (1933), pp. 184–185.

We now choose in our plane E_2 a coordinate system (x, y) such that $p_0=(0, 0)$, $p_n=(1, 0)$. Furthermore, let the open set N contain the open rectangle

$$R: \quad -\epsilon < x < 1+\epsilon, \qquad -\epsilon < y < \epsilon. \tag{3}$$

Finally let $p_i=(x_i, y_i)$. In view of (2) and (3) it suffices to establish the two inequalities

$$-\epsilon < \frac{1}{2^m}\left\{x_i + C_{m,1}x_{i+1} + \cdots + x_{i+m}\right\} < 1+\epsilon, \tag{4}$$

$$-\epsilon < \frac{1}{2^m}\left\{y_i + C_{m,1}y_{i+1} + \cdots + y_{i+m}\right\} < \epsilon, \tag{5}$$

for sufficiently large values of m. From (1), for $m=0$, we get

$$\cdots = x_{-2} = x_{-1} = x_0 = 0, \qquad x_n = x_{n+1} = x_{n+2} = \cdots = 1,$$
$$\cdots = y_{-2} = y_{-1} = y_0 = 0, \qquad y_n = y_{n+1} = y_{n+2} = \cdots = 0.$$

But then our inequalities (4) and (5) obviously hold for sufficiently large values of m, for the sum of any set of at most $n-1$ consecutive ones among the binomial coefficients $1, C_{m,1}, C_{m,2}, \cdots, 1$, divided by their total sum $2^m=1+C_{m,1}+\cdots+1$, tends uniformly to zero as $m\to\infty$. Hence our lemma is proved.[5]

Our geometrical Lemma 2 will be made effective for our purpose by the following third and last lemma which states the effect of the assumption of local convexity on connected sets.

LEMMA 3. *Let M be a set in Hilbert space which is closed, connected and locally convex. Then M is also connected in the following stronger sense: Any two points a and b of M may be joined by a finite polygonal line lying wholly in M.*[6]

Indeed, denote by N the set of points of M which may be joined to the fixed point a by a finite polygonal line lying in M.

[5] A proof of Theorem 2 in the complex Hilbert space requires a proof of Lemma 2 in the k-dimensional complex euclidean (unitary) space U_k. The proof just given is readily adaptable to the space U_2 of two complex coordinates $x=x'+ix''$, $y=y'+iy''$. The only change is that the rectangular neighborhood (3) of the segment $\overline{p_0p_n}$ is to be replaced by the open set defined by $-\epsilon<x'<1+\epsilon$, $-\epsilon<x''<\epsilon$, $-\epsilon<y'<\epsilon$, $-\epsilon<y''<\epsilon$. This is essentially again the real case for the space E_4.

[6] Open connected sets are known to enjoy this stronger connectivity property. In fact Lemma 3 implies this classical property since open sets are locally convex as already mentioned.

Lemma 3 was pointed out to the author by S. Kakutani and J. W. Tukey. The earlier version of this paper was thereby simplified and the method became applicable to Hilbert space.

N is closed in M. Indeed, let $q_i \to q$, $q_i \in N$, $q \in M$. Since $M \cdot S(q; r)$ is convex for a certain $r > 0$, as soon as $q_i \in S(q; r)$ we have $\overline{q_i q} \subset M$, hence $q \in N$.

N is open in M. For if $q \in N$ clearly all points of $M \cdot S(q; r)$ will be in N, provided r is sufficiently small.

The connectedness of M now implies that $N = M$.

3. **Proof of Theorem** 2. Let M be a closed and connected set in H which is also locally convex. Let a and b be any two points of M. We want to show that $\overline{ab} \subset M$. By Lemma 3 there is a sequence of points $p_1, \cdots, p_{n-1}$ such that the polygonal line $\Pi = a p_1 p_2 \cdots p_{n-1} b$ lies in M. Let E_n be a euclidean subspace of H which contains this polygonal line Π. Let furthermore $\overline{S}(a; r)$ be a closed sphere of H of sufficiently large radius r so as to contain our polygonal line Π. The intersection

$$M_1 = M \cdot E_n \cdot \overline{S}(a; r)$$

is obviously closed and bounded, hence also self-compact as being a subset of E_n. But M_1 is also locally convex, being the intersection of three locally convex sets. By Lemma 1 we know that M_1 is δ-convex for some appropriate value of δ. On the other hand our assumptions insure that $\Pi \subset M_1$. By subdividing, if necessary, the sides of Π we may assume that the sides $p_i p_{i+1}$ of the line Π are all of length less than δ. We now perform the construction of Lemma 2. Since $\Pi \subset M_1$, the δ-convexity of M_1 and the triangle inequality imply that also $\Pi' \subset M_1$. Since all sides of all derived polygonal lines $\Pi^{(m)}$ are of length less than δ, induction with respect to m will show that $\Pi^{(m)} \subset M_1$ for all values of m. By Lemma 2 $\Pi^{(m)}$ converges to the segment $\overline{ab}$ as $m \to \infty$. Since M_1 is closed we indeed have $ab \subset M_1$, hence $\overline{ab} \subset M$. Thus M is convex and our theorem is proved.

UNIVERSITY OF PENNSYLVANIA

ON 3-DIMENSIONAL MANIFOLDS

C. E. CLARK

Let P be a 3-dimensional manifold.[1] Let Q be a 2-dimensional manifold imbedded in P. Moreover, let P and Q admit of a *permissible simplicial division* K, that is, a simplicial division of P such that some subcomplex of K, say L, is a simplicial division of Q. Let K_i and L_i denote the ith normal subdivisions of K and L, respectively. We define the *neighborhood* N_i of L_i to be the simplicial complex consisting of the simplexes of K_i that have at least one vertex in L_i together with the sides of all such simplexes. By the *boundary* B_i of N_i we mean the simplicial complex consisting of the simplexes of N_i that have no vertex in L_i. Our purpose is to prove the following theorem.

THEOREM. *The boundary B_2 is a two-fold but not necessarily connected covering of Q, and change of permissible division K replaces B_2 by a homeomorph of itself.*

PROOF. The neighborhood N_1 is the sum of a set of 3-dimensional simplexes. Some of these 3-simplexes, say $a_1, a_2, \cdots$, have exactly one vertex in L_1, others, say $b_1, b_2, \cdots$, have exactly two vertices in L_1, while the remaining, say $c_1, c_2, \cdots$, have three vertices in L_1. Since K_1 is a normal subdivision of K, the intersection of L_1 and b_i or c_i is a 1-simplex or 2-simplex, respectively. Let α_i, β_i, and γ_i be the intersections of B_2 and a_i, b_i, and c_i, respectively. We shall regard α_i and γ_i as triangles with vertices on the 1-simplexes of a_i and c_i. Also we shall regard β_i as a square with vertices on the 1-simplexes of b_i.

Any 2-simplex of L_1, say ABC, is incident to exactly two of the c_i. Let $c_1 = ABCM$. There is a unique 3-simplex of N_1, say σ, that is incident to ABM and different from c_1. This σ is either a c_i, say c_2, or a b_i, say b_2. If σ is c_2, then the triangles γ_1 and γ_2 have a common side. Suppose that σ is $b_2 = ABMN$. The 2-simplex ABN is incident to a unique 3-simplex of N_1, say τ, with $\tau \neq ABMN$. This τ is either c_3 or b_3. If $\tau = b_3$, there is a c_4, or b_4. Finally we must find a $c_p = ABDS$, D in L_1, S in B_1. We now consider $\beta_2, \beta_3, \cdots$, and β_{p-1}. The sum of these squares is topologically equivalent to a square. One side of the square is coincident with a side of γ_1 and the opposite side coincident with a side of γ_p.

Received by the editors July 21, 1941.

[1] Our terminology is that of Seifert-Threlfall, *Lehrbuch der Topologie*. Manifolds are finite, while simplexes and cells are closed point sets.

Since K_1 is a manifold, we can repeat the construction and associate with ABC and ABD a second pair of triangles in B_2 that are either incident along a common side or incident to opposite sides of a square. But there is not a third such configuration associated with ABC and ABD. We repeat the construction for all pairs of adjacent 2-simplexes of L_1. Then to each 2-simplex of L_1 there correspond two triangles in B_2. Moreover, if two 2-simplexes of L_1 are incident along a side, the four corresponding triangles can be paired so that the two triangles of each pair either have a common side or are incident to opposite sides of a square.

Since P and Q are 3- and 2-manifolds, respectively, we can say that Q is two-sided in P in the neighborhood of any point of Q. Moreover, the two γ's of B_2 that correspond to a 2-simplex of L_1 lie on opposite sides of Q (in the neighborhood of this 2-simplex).

Consider a vertex X of L_1 and the 2-simplexes Δ_i of L_1 that have X as a vertex. On one side of Q (in the neighborhood of X) there corresponds to each Δ_i a unique γ_i, and the γ's have the same incidences as the corresponding Δ's (we say that two γ's are incident if they are incident to opposite sides of a square). Let us denote by R the points of these γ's and the squares incident to pairs of these γ's. Let A denote the points of all α_i's that are in a_i's incident to X and on the side of Q that we are considering.

We shall show that $R+A$ is a 2-cell. To do this we shall show that $R+A$ is a manifold relative to its boundary, that its boundary consists of one or more circles, and that any 1-cycle of $R+A$ bounds in $R+A$. First we observe that B_2 is a manifold; this fact follows from the structure of B_2 and the fact that K_1 is a manifold; the argument is elementary and we omit it. Since $R+A$ is the sum of 2-cells α, β, and γ, the set $R+A$ is a manifold relative to its boundary.

To show that this boundary of $R+A$ consists of one or more circles we shall study the incidences among the cells of $R+A$. First, let a_i have X as a vertex. If a 2-dimensional side of a_i is not in B_1, this side must be a side of an a_j or b_j. Furthermore, this a_j or b_j has X as a vertex. Hence, any side of an α_i is also a side of an α_j or β_j of $R+A$. Next, let c_i have vertices $XABM$, M in B_1. The sides of γ_i that are in XAM and XBM are sides of γ_j's or β_j's of $R+A$. But the side of γ_i in ABM is not incident to any other 2-cell of $R+A$. This side is part of the boundary of $R+A$. Finally, let b_i have vertices $XAMN$, A in L_1. The sides of β_i in XAM and XAN are incident to sides of β_j's or γ_j's of $R+A$; the side of β_i in XMN is incident to an α_j or β_j of $R+A$; but the side of β_i in AMN is not incident to any other 2-cell of $R+A$. This side is part of the boundary of $R+A$. Examination of

the segments of the boundary of $R+A$ shows that they fit together to form one or more circles.

We next show that if C is a 1-dimensional cycle of $R+A$, then C bounds in $R+A$. We shall find it convenient to replace A by a new set that will never be empty. We define A' to be A together with all vertices of γ's of R that are not in the boundary of $R+A$ and all sides of squares of R that are not sides of γ's of R and not in the boundary of $R+A$. If A is not empty, the set A' is the same as A. But in any case A' is not empty, and $R+A'$ is the same set as $R+A$. The set $(R+A')-\overline{A}'$ is homeomorphic to a 2-cell with an inner point removed because $(R+A')-\overline{A}'$ can be obtained from the configuration of the 2-simplexes of L_1 that have X as a vertex by removing X and replacing some of the 1-simplexes by squares (open along one side). Hence, the cycle C is homologous in $R+A'$ to a cycle on A', and we assume that C is on A'. The set A' is part of b, the boundary of the combinatorial neighborhood of X in K_2. Since K_2 is a manifold, the set b is a 2-sphere. Assume that C does not bound in A'. Then C must surround a 2-simplex of b that is not in A'. We easily find a 2-simplex of $R+A'$ that is not incident along one of its sides to another 2-simplex of the manifold B_2. This contradiction proves that C bounds, and the proof that $R+A$ is a 2-cell is complete.

Now we draw some lines on $R+A$. If two γ's have a common side, we draw a line coincident with this common side. If two γ's are incident to a square, we draw a line across the square half way between the γ's. All these lines are continued so that they meet at a point of A. These lines give a subdivision of $R+A$ that is combinatorially equivalent to the combinatorial neighborhood of X in L_1. The lines can be drawn for all $R+A$ of B_2 and we get a subdivision of B_2 that is combinatorially equivalent to a two-fold but not necessarily connected covering of L_1.

A triangle of the covering is associated with a 2-simplex of L_1 and a side of Q (in the neighborhood of this simplex). Hence, a homeomorphism is determined between this covering and any covering obtained by changing the permissible division K.

The theorem is not true with B_1 rather than B_2. For example, let Q be the boundary of a 3-simplex of K. Then B_1 is a sphere and a point.

We can prove the following theorem in the same way but with much less effort.

THEOREM. *The above theorem is true if P and Q are replaced by 2- and 1-dimensional manifolds.*

PURDUE UNIVERSITY

A LINEAR TRANSFORMATION WHOSE VARIABLES AND COEFFICIENTS ARE SETS OF POINTS

S. T. SANDERS, JR.

Introduction. While the theory of the linear transformation has been developed in great detail, attention has seldom[1] been called to the transformation T in which variables and coefficients are sets of points. Doubtless the nonexistence of a unique inverse transformation has occasioned this neglect. In this paper the writer studies the iteration of T.

Consider first the transformation

$$T: \quad \begin{aligned} x_1 &= a_{11}x_1' + a_{12}x_2' \\ x_2 &= a_{21}x_1' + a_{22}x_2' \end{aligned},$$

whose *set matrix* is

$$M = \left\| \begin{matrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{matrix} \right\|,$$

where the a's and x's are sets of points, and the indicated sums and products refer to set operations. Applying T to the primed variables, we have the product transformation

$$T^2: \quad \begin{aligned} x_1 &= \overset{(2)}{a}_{11}\, x_1'' + \overset{(2)}{a}_{12}\, x_2'' \\ x_2 &= \overset{(2)}{a}_{21}\, x_1'' + \overset{(2)}{a}_{22}\, x_2'' \end{aligned},$$

of set matrix

$$M^2 = \left\| \begin{matrix} \overset{(2)}{a}_{11} & \overset{(2)}{a}_{12} \\ \overset{(2)}{a}_{21} & \overset{(2)}{a}_{22} \end{matrix} \right\|,$$

where

$$(1) \qquad \begin{aligned} \overset{(2)}{a}_{11} &= a_{11} + a_{12}a_{21}, & \overset{(2)}{a}_{12} &= a_{11}a_{12} + a_{12}a_{22}, \\ \overset{(2)}{a}_{21} &= a_{21}a_{11} + a_{22}a_{21}, & \overset{(2)}{a}_{22} &= a_{21}a_{12} + a_{22}. \end{aligned}$$

Transforming in turn each new set of variables, we obtain product transformations T^3, T^4, $\cdots$, whose set matrices are M^3, M^4, $\cdots$.

Presented to the Society, December 30, 1941 under the title *On powers of a matrix whose elements are sets of points;* received by the editors August 25, 1941.

[1] Lowenheim, *Über Transformationen im Gebietekalkül*, Mathematische Annalen, vol. 73 (1913), pp. 245–272; *Gebietsdetermination*, Mathematische Annalen, vol.79 (1919), pp. 223–236.

Set matrices $M(a_{ij})$ and $M'(a'_{ij})$ are defined to be *equal* if $a_{ij}=a'_{ij}$, $i, j=1, 2, \cdots, n$, while if $a_{ij} \subset a'_{ij}$,[2] then we shall write $M \subset M'$. A sequence M_k, $k=1, 2, \cdots$, of set matrices is *increasing* or *decreasing* according as $M_k \subset M_{k+1}$, or $M_{k+1} \subset M_k$.

From (1) follow $a_{11} \subset a_{11}^{(2)}$ and $a_{22} \subset a_{22}^{(2)}$. The assumptions $a_{12} \subset a_{12}^{(2)}$ and $a_{21} \subset a_{21}^{(2)}$ are equivalent to

$$a_{12} + a_{21} \subset a_{11} + a_{22}, \tag{2}$$

which is a necessary and sufficient condition that $M \subset M^2$. But from (1) we have $a_{12}^{(2)}+a_{21}^{(2)} \subset a_{11}^{(2)}+a_{22}^{(2)}$, whence by (2) the inclusion $M^2 \subset M^4$, and the following theorem is established.

THEOREM 1. *The sequences M^{2k} and M^{2k+1}, $k=1, 2, \cdots$, of second order set matrices are increasing.*

From (1) follow also $a_{12}^{(2)} \subset a_{12}$ and $a_{21}^{(2)} \subset a_{21}$, while the assumptions $a_{11}^{(2)} \subset a_{11}$ and $a_{22}^{(2)} \subset a_{22}$ are equivalent to

$$a_{12}a_{21} \subset a_{11}a_{22}, \tag{3}$$

a necessary and sufficient condition that $M^2 \subset M$. From (1) comes $a_{12}^{(2)}a_{21}^{(2)} \subset a_{11}^{(2)}a_{22}^{(2)}$, whence by (3) the inclusion $M^4 \subset M^2$, and the following theorem.

THEOREM 2. *The sequences M^{2k} and M^{2k+1}, $k=1, 2, \cdots$, of second order set matrices are decreasing.*

This theorem follows at once.

THEOREM 3. *Even powers of a second order transformation are identical; likewise odd powers beyond the first.*

The general case. Consider the transformation

$$T: \quad x_i = \sum_{j=1}^{n} a_{ij}x'_j, \qquad i = 1, 2, \cdots, n,$$

of set matrix

$$M = \left\| \begin{matrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ \cdot & \cdot \quad \cdots \cdot \\ a_{n1} & a_{n2} \cdots a_{nn} \end{matrix} \right\|,$$

where the variables and coefficients are sets of points in a space whose generality is limited only by the following assumption.

[2] The symbol $\subset$ denotes inclusion.

(A) *The elements a_{ij} of M are independent point sets.* That is, if products $P_1, P_2, \cdots, P_k, \cdots$ of elements of M are such that

$$P_1 \subset \sum_{k \neq 1} P_k,$$

there is a subscript $k = k'$ such that[3] $P_1 \subset P_{k'}$.

The following theorem will presently be established.

THEOREM 4. *The iteration of the transformation T of order n leads to at most $(n-1)^2+N$ distinct transformations, where N is the least common multiple of $1, 2, \cdots, n$, and at most N of these transformations recur periodically. If the coefficients of T are independent, there are precisely $(n-1)^2+N$ distinct transformations of which N recur periodically.*

We shall denote by $a_{ij}^{(p)}$ the element in the ith row and jth column of M^p. Clearly $a_{ij}^{(p)}$ is a sum of products of the form

$$P = a_{ik_2}a_{k_2k_3}a_{k_3k_4} \cdots a_{k_pj},$$

for all distinct ways of selecting the subscripts $k_2, k_3, \cdots, k_p$, from the integers $1, 2, \cdots, n$. The characteristic interlocking form k_rk_s, k_sk_t of the subscripts of consecutive factors of P will be expressed in the word *proper*. Thus $a_{13}a_{32}a_{23}a_{32}a_{22}$ is a term of $a_{12}^{(5)}$ and a proper product, as opposed to the identical point set $a_{13}a_{32}a_{23}a_{22}$.

The *order* of a product P is the number of factors occurring in the product. The orders of products $P, C, \cdots$, will be denoted by $p, c, \cdots$. A *cycle* of P is a proper product $a_{k_1k_2}a_{k_2k_3} \cdots a_{k_ck_1}$ of factors of P in which the subscripts $k_1, k_2, \cdots, k_c$ are distinct. It is convenient to denote such a cycle by C_{k_1}. Thus $a_{12}a_{23}a_{33}a_{32}$ involves the cycles $C_2 = a_{23}a_{32}$, $C_3 = a_{33}$, and $C_3' = a_{32}a_{23}$. A *closed cycle* of P is one whose factors occur consecutively in P. A product P is *c-cyclic* if every product of c consecutive factors is a closed cycle. It follows that these closed cycles are cyclic permutations of a single cycle C, known as the defining cycle of the product P. Thus $a_{23}a_{31}a_{12}a_{23}a_{31}$ is 3-cyclic, with the defining cycle $C_2 = a_{23}a_{31}a_{12}$.

Proper products are *coterminal* if corresponding terminal subscripts are equal. Thus $P = a_{12}a_{23}a_{34}$ and $P_1 = a_{15}a_{54}$ are coterminal. Such products clearly are terms of elements similarly situated in set matrices M^p and $M^{p'}$. It is convenient to denote a proper product $a_{ik_2}a_{k_2k_3} \cdots a_{k_pj}$ by P_{ij}. If coterminal proper products P_{ij}, P_{ij}' are

[3] Thus, under (A), such inclusions as $a_{12}a_{23} \subset P = a_{14}+a_{13}a_{32}$ cannot hold, since P does not involve one of the terms a_{12}, a_{23}, $a_{12}a_{23}$.

such that $p'_{ij}<p_{ij}$ while $P_{ij}\subset P'_{ij}$, we say that P'_{ij} is a *contraction* of P_{ij}, while P_{ij} is an *expansion* of P'_{ij}. Thus $a_{13}a_{22}$ is a contraction of $a_{12}a_{24}a_{42}a_{23}$, while the latter product is an expansion of the former.

The following lemmas are immediate consequences of the preceding definitions.

LEMMA 1. *A proper product of order exceeding $n-1$ involves a closed cycle.*

LEMMA 2. *The deletion of a closed cycle from a proper product of greater order yields a contraction of the product.*

LEMMA 3. *The insertion of a cycle C_{k_s} into a proper product immediately following a factor $a_{k_rk_s}$, or immediately preceding a factor $a_{k_sk_t}$, yields an expansion of the product. Thus the appropriate insertion of $C_1=a_{14}a_{41}$ into $P_{12}=a_{12}a_{31}a_{12}$ yields $P'_{12}=a_{12}a_{31}a_{14}a_{41}a_{12}$, or $a_{14}a_{41}a_{12}a_{31}a_{12}$.*

Consider the sequence

$$P_{ij},\ P'_{ij},\ P''_{ij},\ \cdots,\ P^{(k)}_{ij}, \tag{4}$$

in which each element after the first is obtained from its predecessor by the deletion of a closed cycle. The last element can involve no cycle, or is itself a cycle, and is called a *stem* of P_{ij}. The definition is not unique, since $P^{(k)}_{ij}$ clearly varies with the sequence of cycles of P_{ij} whose deletion leads to (4). Thus $a_{12}a_{23}a_{32}a_{24}a_{43}$ has the stems $a_{12}a_{22}$ and $a_{12}a_{24}a_{43}$.

From Lemmas 1 and 2 follows this lemma.

LEMMA 4. *A stem of a proper product P is a contraction of P which has no contraction. The order of a stem cannot exceed n.*

Increasing sequences. We first prove this lemma.

LEMMA 5. *For every integer c not exceeding p nor n, there occurs in M^p, $p\geqq 2$, an element involving a term which is a c-cyclic product.*

If $p=mc$ each diagonal element $a^{(p)}_{ii}$ involves certain c-cyclic terms in which a cycle C is repeated m times. If $p=mc+r$, $1\leqq r<c$, each element $a^{(p)}_{ij}$, $i\neq j$, involves certain c-cyclic terms in which the rth factor, and hence the pth, is a_{kj}. Thus, for $n\geqq 4$, $a^{(4)}_{33}$ involves the 2-cyclic term $a_{31}a_{13}a_{31}a_{13}$, while $a^{(5)}_{24}$ involves the 3-cyclic term $a_{21}a_{14}a_{42}a_{21}a_{14}$.

THEOREM 5. *Let M be a set matrix of order n whose elements are independent. The sequence $M^{p_1}, M^{p_2}, \cdots, M^{p_r}, M^{p_{r+1}}, \cdots$, $p_r<p_{r+1}$, is increasing if and only if $p_1>n-1$, while $p_{r+1}-p_r$ is a multiple of $1, 2, \cdots, n$.*

By Lemma 1 a term P of $a_{ij}^{(p_r)}$ involves a closed cycle C. Since $p_{r+1}-p_r$ is a multiple of c we can insert appropriately into P sufficient repetitions of C to yield by Lemma 3 an expansion $\overline{P}=P$ of order p_{r+1}. Thus $\overline{P}$ is the required term of $a_{ij}^{(p_{r+1})}$.

Conversely, if $p_1 \leqq n-1$ there is a term P' of $a_{ij}^{(p_1)}$ involving no cycle, and which by Lemma 1 and (A) is not contained in $a_{ij}^{(p)}$ for $p=p_2 \geqq n$. And if $p_1>n-1$ while $p_{r+1}-p_r$ is not a multiple of $c \leqq n$, there is by Lemma 5 an element $a_{ij}^{(p_r)}$ of M^{p_r} involving a term P_r which is a c-cyclic product. Now a product P_{r+1} which contains P_r can by (A) involve only factors of P_r, and is hence c-cyclic. But since $p_{r+1}-p_r$ is not a multiple of c, it follows that P_{r+1} is not coterminal with P_r, and so is not a term of $a_{ij}^{(p_{r+1})}$. From (A) we conclude that P_r is not contained in the set $a_{ij}^{(p_{r+1})}$ and the theorem is established.

Decreasing sequences. Before proceeding we prove two lemmas.

LEMMA 6. *Let P be a proper product, S a sequence of cycles of P determining a stem P', $h=h(S)$ the highest common factor of the orders of the cycles of S, and c the greatest of these orders. There is a contraction $\overline{P}$ of P involving every subscript of P, and such that $\bar{p} \leqq c(n-c+2)-1$, $p \equiv \bar{p} \pmod{h}$.*

Consider the following sequence

$$S': \quad P', C_1, C_2, \cdots, C_k,$$

in which: (i) C_1 is a cycle of S involving a subscript not found in P', and has the maximum order of all such cycles. (ii) Each C following C_1 is a cycle of S involving a subscript which has previously appeared in S', and one which has not done so. Further, all such cycles of S are in the sequence S'.

It is easily shown that every subscript involved in P occurs in some cycle of S'. For let k_s be the first subscript of P not found in S'. Since k_s cannot occur in the stem P', it must first appear in P in a factor of the form $a_{k_r k_s}$. But k_s occurs in some cycle C' of S, while k_r occurs in a cycle of S'. We infer from (ii) that C' is a cycle of S', and a contradiction is reached.

Now if the cycles $C_1, C_2, \cdots, C_k$ exist, at least one involves a subscript of P'; for the contrary assumption leads to a contradiction, as in the above argument, on consideration of the first appearance in P of a subscript of $C_1, C_2, \cdots, C_k$. It follows that the cycles of S' can be combined with P' into a contraction $\overline{P}$ of P which involves every subscript of P.

Consider now the order of $\overline{P}$. We have

$$\bar{p} = p' + \sum_{t=1}^{k} c_t, \qquad c_t \leqq c.$$

If $p' \leqq c-2$, P' and C_1 together involve at least c distinct subscripts, whence $k \leqq n-c+1$, and $\bar{p} \leqq c-2+c(n-c+1) < c(n-c+2)-1$. While if $p' > c-2$, P' and C_1 together involve at least $p'+1$ distinct subscripts, whence $k \leqq n-p'$, and $\bar{p} \leqq p'+c(n-p') = cn-p'(c-1) \leqq cn-(c-1)^2 = c(n-c+2)-1$.

The congruence $p \equiv \bar{p} \pmod{h}$ follows from the definition of P' and $\bar{P}$. The lemma is established.

LEMMA 7. *Let $c_1 > c_2 > \cdots > c_m$ be a set S_1 of positive integers whose highest common factor is $h = h(S_1)$. The equation $c_1x_1 + c_2x_2 + \cdots + c_mx_m = k$ has a non-negative integral solution $(x_1', x_2', \cdots, x_m')$ for every integer k which is a multiple of h exceeding $(c_1c_2/h) - c_1 - c_2$.*[4]

THEOREM 6. *Let M be a set matrix of order n whose elements are independent. The sequence $M^{p_1}, M^{p_2}, \cdots, M^{p_r}, M^{p_{r+1}}, \cdots$, $p_r < p_{r+1}$, is decreasing if and only if $p_1 > (n-1)^2$, while $p_{r+1} - p_r$ is a multiple of $1, 2, \cdots, n$.*

Sufficiency. For any term P of $a_{ij}^{(p_{r+1})}$; the theorem asserts the existence of a term P_1 of $a_{ij}^{(p_r)}$ such that $P \subset P_1$. Our procedure is to insert into a contraction of P appropriate cycles of P of the precise total order required to yield the desired product P_1.

Let P' be a stem of P, determined by a sequence S of cycles of P. Let $\bar{P}$ be the contraction of P presented in Lemma 6; and let $S_1: C_1, C_2, \cdots, C_m$, be cycles of S among whose orders, $c_1 > c_2 > \cdots > c_m$ occur all orders of cycles of S. If $m = 1$, the required term P_1 is clearly encountered in the sequence (4) of products defining P'.

Case 1. $c_1 < n$.

By Lemma 6 we have

$$p_r - \bar{p} > (n-1)^2 - c_1(n - c_1 + 2) + 1$$
$$= c_1(c_1 - 1) - c_1 - (c_1 - 1) + (n-1)(n - c_1 - 1),$$

whence

$$(5) \qquad p_r - \bar{p} > c_1(c_1 - 1) - c_1 - (c_1 - 1) \geqq \frac{c_1c_2}{h} - c_1 - c_2.$$

Now by the same lemma, $p_{r+1} - \bar{p} \equiv 0 \pmod{h}$, hence from $p_{r+1} - p_r \equiv 0 \pmod{h}$ follows

[4] This lemma is readily established by mathematical induction. However, a better bound on k, namely, $(c_1 c_m/h) - c_1 - c_m$ has been communicated to the author by Dr. Alfred Brauer.

(6) $$p_r - \bar{p} \equiv 0 \pmod{h}.$$

By (5), (6), and Lemma 7 there is established the existence of non-negative integers, $x_1', x_2', \cdots, x_m'$ such that

$$\bar{p} + \sum_{i=1}^{m} c_i x_i' = p_r.$$

By Lemmas 6 and 3 we can insert the cycles $C_1, C_2, \cdots, C_m$ into $\overline{P}$ and obtain the required product P_1.

Case 2. $c_1 = n$, $c_2 < n-1$.

Again by Lemma 6

$$p_r - \bar{p} > (n-1)^2 - c_1(n - c_1 + 2) + 1$$
$$= c_1(c_1 - 2) - c_1 - (c_1 - 2) + (n-2)(n - c_1),$$

whence

$$p_r - \bar{p} > c_1(c_1 - 2) - c_1 - (c_1 - 2) \geqq \frac{c_1 c_2}{h} - c_1 - c_2,$$

and the proof proceeds as in Case 1.

Case 3. $c_1 = n$, $c_2 = n-1$.

Here the contraction P', instead of $\overline{P}$, is employed. We have by Lemma 4

$$p_r - p' > (n-1)^2 - n = c_1 c_2 - c_1 - c_2.$$

Since $h = 1$ it follows by Lemma 7 that non-negative integers, x_1', x_2', exist such that $p' + c_1 x_1' + c_2 x_2' = p_r$. Thus since P' must involve a subscript of C_1 and C_2, it is possible to insert the cycles C_1, C_2, into P' and obtain by Lemma 3 the required product P_1.

Necessity. As in Theorem 5 it can be shown that $p_{r+1} - p_r$ must be a multiple of $1, 2, \cdots, n$; while for the condition $p_1 > (n-1)^2$, it will suffice to produce a term of an element of M^{p_2} which is not contained in the corresponding element of M^{p_1}, although $p_2 - p_1$ is a multiple of $1, 2, \cdots, n$.

Consider the n-cyclic product P_1' of order $p_1 + n - 1$ whose defining cycle is $C_1 = a_{12}a_{23} \cdots a_{n1}$, and the $(n-1)$-cyclic product P_2' of order $p_2 - p_1 - n + 1$ whose defining cycle is $C_2 = a_{23}a_{34} \cdots a_{n2}$. By inserting P_2' into P_1' following any factor a_{12}, a proper product P of order p_2 is obtained which is a term of an element of the first row of M^{p_2}. Now from (A) and the structure of P it follows that any proper co-terminal product containing P can be had from P by deletion of the cycles C_1, C_2. We are thus led to the equation

(7) $$nx_1 + (n-1)x_2 = p_2 - p_1,$$

with the restrictions

$$nx_1 \leqq p_1 + n - 1, \tag{8}$$

$$(n-1)x_2 \leqq p_2 - p_1 - n + 1. \tag{9}$$

By (7) and (9), x_1 is a positive multiple of $n-1$, while from $p_1 \leqq (n-1)^2$ we have by (8), $nx_1 \leqq n(n-1)$. Thus $x_1 = n-1$, but it is clear that the deletion of $n-1$ cycles C_1 from P will yield a product[5] whose first factor is a_{23}. From (A) it follows that P is not contained in the corresponding element of M^{p_1}, and the theorem is established.

Equality of matrices. Theorems 5 and 6 provide conditions for increase and decrease, respectively, in a sequence of ascending powers of M. In summation we have the following theorem:

THEOREM 7. *Let M be a set matrix of order n whose elements are independent. The equality $M^{p_1} = M^{p_2}$, $p_2 > p_1$, holds if and only if $p_1 > (n-1)^2$, while $p_2 - p_1$ is a multiple of $1, 2, \cdots, n$.*

Theorem 4 is an immediate consequence.

SOUTHWESTERN LOUISIANA INSTITUTE

[5] Thus for $n=3$, $p_1=4$, $p_2=10$, we have $P = a_{12}a_{13}a_{22}a_{23}a_{32}a_{21}a_{31}a_{12}a_{13}a_{31}$ which has no contraction of order 4.

A THEOREM ON LIE GROUPS

DEANE MONTGOMERY AND LEO ZIPPIN

It is the purpose of this note to prove the following theorem:

THEOREM 1. *Let G be a Lie group*[1] *and G^* a compact subgroup of G. Then there exists in G an open set O containing G^* with the property that for each subgroup H of G lying in O there is an element g of G such that $g^{-1}Hg$ is in G^*.*

Roughly, the theorem says that each subgroup near enough to G^* can be transformed into G^* by an appropriate element of G. This result can be regarded as a generalization of the known fact that Lie groups cannot have arbitrarily small subgroups (other than the identity), although it was not from this point of view that our interest arose. To make our meaning clear, assume that G^* is an invariant subgroup so that the factor group G/G^* is also a Lie group. If there were in G a subgroup H near G^* it would go, by the homomorphism taking G into G/G^*, into a subgroup near the identity of G/G^*. The only subgroup of G/G^* near the identity is the identity itself which means that if H is to be near G^* it must actually be a subgroup of G^*. We see that when G^* is an invariant compact subgroup of G, the conclusion of the theorem is true in a trivial sense.

Our proof of Theorem 1 in the more general situation is based on certain facts about the way in which G operates on the coset space G/G^* which will be denoted by M. This is the space whose points are the cosets gG^* of G^* in G. The group G acts transitively on M which can be regarded as a Riemannian space and Cartan[2] has shown that there exists in M a Riemannian metric for which G is a group of isometries. This fact will be of great importance in what follows.

We begin, as we may, by supposing that M is endowed with a Riemannian metric invariant under G and, furthermore, we assume that M has been made into a metric space (Fréchet) in the usual way

---

Presented to the Society, September 5, 1941; received by the editors August 29, 1941.

[1] For all definitions and theorems on topological groups used in this paper see Pontrjagin, *Topological Groups*. The term compact, as used here, implies that the set is closed.

[2] *La Théorie des Groupes Finis et Continus et l'Analysis Situs*, Mémorial des Sciences Mathématiques, vol. 42, p. 43. For an excellent summary of properties of isometries and geodesics which will be useful here, see the paper by Myers and Steenrod, *The group of isometries of a Riemannian manifold*, Annals of Mathematics, (2), vol. 40 (1939), pp. 400–416.

by letting the distance $d(x, y)$, between two points x and y be the greatest lower bound of the lengths of geodesic paths joining a and b. This distance is invariant under G. Moreover, for small enough neighborhoods this distance is equal to the length of the geodesic joining x and y since in such neighborhoods geodesics furnish a proper absolute minimum for the lengths of paths.

We shall use the symbol $S(x, r)$, x a point of M and r a positive real number, to designate the set of points of M whose distance from x is at most r, and we shall call that set the sphere about x of radius r. The boundary of this sphere will be the set of points for which the distance is precisely r, the *inside* (or *interior*) will be the set for which the distance is less than r. We shall say that a sphere is *convex* if each pair of its points are the end points of a geodesic every inner point of which is *inside* the sphere. It will be worth keeping in mind that, on our definition, when a geodesic belongs to a convex sphere only its end points can belong to the boundary of the sphere.

It will be convenient to use a number of simple lemmas and we now turn to them.

LEMMA 1. *If x is any point of M there exists a neighborhood U of x such that if a, b, and c are three distinct points of U which lie on one geodesic in that order, then*

$$d(b, x) < \max [d(a, x), d(c, x)].$$

Let r be a positive number such that every sphere of center x and radius $r' \leqq r$ is convex.[3] Let U be the interior of $S(x, r)$. If a, b, and c are in U, consider the sphere $S(x, r_1)$ where $r_1 = d(x, b)$. The boundary of this sphere meets the geodesic abc at b and this means that either a or c is outside $S(x, r_1)$ as otherwise the fact of convexity of $S(x, r_1)$ would be contradicted. But if a point is outside $S(x, r_1)$ its distance from x is greater than r, and this concludes the proof.

LEMMA 2. *If x is any point of M, there exists a neighborhood U of x such that if a, b, c, and e are four distinct points in U and a, b, and c are on a geodesic in that order then*

$$d(b, e) < \max [d(a, e), d(c, e)].$$

Here we shall let U designate the interior of $S(x, r/2)$ where r has the same meaning as in the preceding lemma. Since G is transitive over M there will be an element g in G such that $g(e) = x$. The points

[3] For the existence of such a number r in a Riemann space see the article by Whitehead, *Convex regions in the geometry of paths*, Quarterly Journal of Mathematics, vol. 3 (1932), pp. 33–42.

$g(a)$, $g(b)$, and $g(c)$ are inside $S(x, r)$, and they are on a geodesic since the isometry g preserves geodesics. Making use of Lemma 1, and using again the fact the g is an isometry, we complete the proof of this lemma.

LEMMA 3. *If x is a point of M there is a neighborhood U of x such that if a, b, c are distinct points lying in that order on a geodesic in U and if d, e, f are distinct and lie in that order on a geodesic in U then*

$$d(b, e) < \max [d(a, d), d(a, f), d(c, d), d(c, f)].$$

First we conclude from Lemma 2 that $d(b, e)$ is either less than $d(a, e)$ or less than $d(c, e)$. Say the notation is such that

$$d(b, e) < d(a, e).$$

Now using Lemma 2 again we have

$$d(a, e) < \max [d(a, d), d(a, b)],$$

and Lemma 3 is proved.

LEMMA 4. *If x is any point in M, there exists a neighborhood U of x such that if H is a closed subgroup of G and $H(x)$[4] is in U then H has a fixed point in U.*

Let U denote some convex sphere about x which satisfies the conclusion of Lemma 3. We shall show that this U fulfills the conclusion of the present lemma. Suppose, therefore, that H is a subgroup of G such that $H(x)$ is contained in $\overline{U}$.

Let q be a point in $\overline{U}$ such that $H(q)$ is of minimum diameter with respect to all orbits of H which lie entirely in $\overline{U}$. If $H(q) = q$ our proof is completed so we may take it that $H(q) \neq q$.

In this case $H(q)$ contains at least two points. Let b denote the midpoint of some geodesic determined by a pair of points of $H(q)$; now, because H is a group of isometries, $H(b)$ is entirely included in the set of such midpoints, and $H(b)$ lies in U. It will now be shown that $H(b)$ has a smaller diameter than $H(q)$ and this will be a contradiction to our choice of q. This contradiction will complete the proof of our lemma.

The diameter of $H(b)$ coincides with the distance between two points of $H(b)$. This implies that there is an h in H such that the diameter of $H(b)$ is

$$d[b, h(b)].$$

[4] This is the orbit of the point x under the group H.

The point b is the midpoint of a geodesic abc where a and c are in $H(q)$. The point $h(b)$ is on the geodesic $h(a)$, $h(b)$, $h(c)$. Calling these points d, e, and f we may apply Lemma 3 and conclude that

$$d[b, h(b)] < \max\{d[a, h(a)], d[a, h(c)], d[c, h(a)], d[c, h(c)]\}.$$

This shows that the diameter of $H(b)$ is smaller than that of $H(q)$ and completes the proof of this lemma.

It is now a simple matter to conclude the proof of our theorem. We have to recall that the "points" of the space M are the cosets gG^*, g in G. Let us now interpret Lemma 4 in this light, with the group G^* taken as the point x. The open set U of the lemma corresponds to a system of cosets gG^* and the set of elements of G which belong to one of these cosets constitutes an open set O of G. The set O is a neighborhood of G^*.

Now let H be a subgroup of G which lies in O and let h be an element of H. Then, by the construction of O, every element of the coset hG^* belongs to O and the point hG^* of M belongs to U in M. Therefore the premises of Lemma 4 are satisfied and we may suppose that H has a fixed point in M.

This means that there is a "point" gG^* of M such that

$$H(gG^*) = gG^*.$$

This, however, is an equation in sets in G. We may write it

$$HgG^* = gG^*.$$

From this we conclude that

$$g^{-1}HgG^* = G^*.$$

But this means that for every choice of an element k in G^* and element h in H: $g^{-1}hgk$ is contained in G^*.

This means that for every choice of h in H: $g^{-1}hg$ is contained in G^* and then finally, that the group $g^{-1}Hg$ is a subgroup of G^*. This concludes the proof of our theorem.

COROLLARY. *The element g of Theorem 1 may be chosen within any prescribed neighborhood of the identity if the open set O is chosen thereafter sufficiently small.*

This corollary is a consequence of our method of proof. If the neighborhood U of the last lemma is small H will have a fixed point y near x. Because of the transitivity of G over M there is a g in G such that $g = g(x)$ and this g may be chosen near the identity in G if y is near enough to x.

These results may be extended slightly in certain directions as follows:

THEOREM 2. *Let G be a compact connected finite-dimensional group and let G^* be a closed connected subgroup. There exists an open set O containing G^* such that if H is a closed connected group in O then H is the transform of a subgroup of G^*.*

Let Z be an invariant zero-dimensional subgroup of G such that $f(G)=G/Z$ is a Lie group. By Theorem 1 there exists an open set O_1 containing $f(G^*)$ such that any subgroup of $f(G)$ which is in O_1 can be transformed into a subgroup of $f(G^*)$. Let $O=f^{-1}(O_1)$, and let H be a closed connected subgroup of G which is contained in O. There is a g_1 in $f(G)$ such that $g_1^{-1}f(H)g_1$ is in $f(G^*)$. Let g be an element in $f^{-1}(g_1)$. Then $g^{-1}Hg$ is a connected group such that $f(g^{-1}Hg)$ is in $f(G^*)$. This means that every element of $g^{-1}Hg$ belongs to the collection of elements $G^*Z=f^{-1}f(G^*)$.

The set of elements G^*Z forms a group which must have the same dimension as G^* for both are taken by f into $f(G^*)$ and the homomorphism f, since it has a zero-dimensional kernel, preserves dimension.[5] Hence the component of the identity of G^*Z must be G^*. For in any case this component certainly includes G^* and it cannot be larger than G^*, because if a finite-dimensional connected compact group contains another connected closed group as a *proper* subgroup it must be of higher dimension than this subgroup. This fact can be seen generally by observing that a similar fact is true for Lie groups.

If the connected group $g^{-1}Hg$ is in G^*Z it must be in the component of the identity of G^*Z. Therefore $g^{-1}Hg$ is in G^* as we wished to prove.

SMITH COLLEGE AND
QUEENS COLLEGE

[5] See van Kampen, *Note on a theorem of Pontrjagin*, American Journal of Mathematics, vol. 58 (1936), pp. 177–180, especially p. 178.

A NOTE ON COMPLEMENTATION IN LATTICES

L. R. WILCOX

The results of this note concern the notions of complementation and modularity in lattices. In the theories of modular lattices, for example, the theory of continuous geometries of von Neumann, the assumption of complementation has proved extremely powerful; the author has found that some analogue of this assumption is usually necessary in the study of non-modular lattices.[1] If L is a modular lattice with 0, 1, and if $a \in L$, then x is a complement of a in case $a+x=1$, $ax=0$. If L has the property

(1) each $a \in L$ has a complement,

then it may be proved that

(2) $a, b \in L$ implies the existence of $b_1 \leqq b$ such that

$$a + b_1 = a + b, \qquad ab_1 = 0.$$

Property (2) is the really useful one. Now if L is any lattice with 0, 1, then (1) does not imply (2); moreover, even (2) seems too weak for most purposes. However, if in (2) we assume in addition that (a, b_1) (or (b_1, a)) is a modular pair, then the usefulness of this assumption in analyzing the structure of L is considerably increased. At the same time, of course, limitations are placed on L, and it is these which we study here.

Let L be a lattice with 0 and 1. If $b, c \in L$, we say that (b, c) is a *modular pair* and write $(b, c)M$ if $(a+b)c=a+bc$ for $a \leqq c$. We write $(b, c) \perp$ if $bc=0$ and $(b, c)M$. The negation of M is M'. If $bc=0$ and $(b, c)M'$ we write $b \| c$. If $\perp$ is a symmetric relation, L is said to be *$\perp$-symmetric*; if M is symmetric, L is said to be *M-symmetric*.[2]

DEFINITION 1. *Let $a, b, b_1 \in L$. Then b_1 is a right complement within b of a in $a+b$ if*

$$b_1 \leqq b, \qquad a + b_1 = a + b, \qquad (a, b_1) \perp.$$

We say that b_1 is a left complement within b of a in $a+b$ if

$$b_1 \leqq b, \qquad a + b_1 = a + b, \qquad (b_1, a) \perp.$$

If $a \leqq b$, the phrase "within b" is omitted; if $a+b=1$, the phrase

Presented to the Society, September 5, 1941; received by the editors September 24, 1941.

[1] This Bulletin, abstract 47-5-208

[2] See L. R. Wilcox, *Modularity in the theory of lattices*, Annals of Mathematics, (2), vol. 40 (1939), pp. 490–505, for the elementary properties of the relations M and $\perp$.

"in $a+b$" is omitted. L is right (left) complemented if $a, b \in L$ implies the existence of b_1 such that b_1 is a right (left) complement within b of a in $a+b$. If L is $\perp$-symmetric, right and left complements coincide, and the words "right" and "left" will be omitted.

THEOREM 1. *Let $(a, b)M$. Then b_1 is a right complement within b of a in $a+b$ if and only if b_1 is a right complement of ab in b. The forward implication holds also for left complements.*

PROOF. Suppose $b_1 \leqq b$, $b_1+a=b+a$, $(a, b_1) \perp$ (or $(b_1, a) \perp$). Then

$$b_1 + ab = (b_1 + a)b = (b + a)b = b;$$

$(ab, b_1) \perp$ (or $(b_1, ab) \perp$) is immediate. Suppose that $ab+b_1=b$, $(ab, b_1) \perp$. Then $b_1 \leqq b$; moreover, $a+b_1=a+ab+b_1=a+b$. Clearly $ab_1=abb_1=0$. Let $d \leqq b_1$, whence

$$\begin{aligned}(d + a)b_1 &= (d + a)bb_1 = (d + ab)b_1 \\ &= d + abb_1 = d + ab_1,\end{aligned}$$

and $(a, b_1)M$. Hence $(a, b_1) \perp$, and b_1 is a right complement within b of a in $a+b$.

We turn now to consequences of the assumption that L is left complemented. The fundamental result follows.

THEOREM 2. *If L is left complemented, then L is right complemented, the notions of right and left complement coincide, and L is M-symmetric.*

PROOF. Let $(b, c)M$. There exists a left complement c_1 within c of b in $b+c$. Now let $b_1 \leqq b$. Then by the second part of Theorem 1 c_1 is a left complement of bc in c, and

$$(b_1 + c)b = (b_1 + bc + c_1)b = b_1 + bc,$$

whence $(c, b)M$. The remainder of the theorem is immediate.

COROLLARY. *If L is $\perp$-symmetric and complemented, then L is M-symmetric.*

REMARK. It is false that if L is right complemented then L is left complemented. For, in the right complemented lattice consisting of 0, 1, three points p, q, r, and a line s with $s > p, q$ but $s \not> r$, the element s has no left complement (in 1).

We shall henceforth assume that L is left complemented. It is now possible to prove a converse of Theorem 1.

THEOREM 3. *Let $a, b \in L$. If every complement b_1 within b of a in $a+b$ is a complement of ab in b, then $(a, b)M$.*

PROOF. Let $d \leqq b$, and let d_1 be a complement within d of a in $a+d$. Then

$$d_1 + a = d + a, \qquad (d_1, a) \perp.$$

Now let b' be a complement within b of $d+a$ in $b+a$. Then

$$b' + d_1 + a = b' + d + a = b + a;$$

moreover, $(b', d+a) \perp$, whence $(b', d_1, a) \perp$, and $(b'+d_1, a) \perp$. Define $b_1 \equiv b'+d_1$. Then $b_1 \leqq b$, $b_1+a = b+a$, $(b_1, a) \perp$, that is, b_1 is a complement within b of a in $a+b$. By the hypothesis, b_1 is a complement of ab in b, whence $b_1+ab = b$. Now

$$\begin{aligned}(d + a)b &= (d + a)(b_1 + ab) \\ &= ((ab + d_1) + b')(d + a) \\ &= ab + d_1 \leqq d + ab\end{aligned}$$

since $ab+d_1 \leqq d+a$, $(b', d+a) \perp$. But $d+ab \leqq (d+a)b$, whence $(d+a)b = d+ab$, and $(a, b)M$.

COROLLARY 1. *$(a, b)M$ if and only if every complement within b of a in $a+b$ is a complement of ab in b.*

COROLLARY 2. *$(a, b)M'$ if and only if there exists a complement b_1 within b of a in $a+b$ such that $b_1+ab < b$.*

COROLLARY 3. *$a \| b$ if and only if $ab = 0$ and there exists $b_1 < b$ such that $b_1+a = b+a$ and $(b_1, a) \perp$.*

REMARK. It should be observed that Corollary 3 justifies our use of the symbol $\|$. Let, for example, L be a euclidean (or affine) geometry. Parallel spaces in L are then characterized by the condition $ab = 0$ and the existence of a space $b_1 < b$ such that $b_1+a = b+a$; if b_1 is chosen as a minimal space with these properties, and it can be so chosen, then $(b_1, a) \perp$.

It is easily seen[3] that an affine geometry is a left complemented lattice. Indeed, it may be shown that the property

$$(3) \qquad bc \neq 0 \quad \text{implies} \quad (b, c)M$$

holds in an affine geometry. Property (3) may be stated also in the following way. Define the set M_L' as the set $[bc; (b, c)M']$. Then

$$(3') \qquad M_L' \subset [0].$$

It is of interest to investigate the nature of the set M_L' for our general

[3] L. R. Wilcox, loc. cit., pp. 496–499.

left complemented lattice L. It might appear that M_L' is an ideal; that this is false will be shown by an example. However, the next theorem shows that M_L' has one of the properties of an ideal.

LEMMA 1. *Let $(b, c)M'$ and $a<bc$. Then there exists $b'<b$ with $a=b'c$ and $(b', c)M'$. Moreover, there exists $x\leqq b$ with $x\|c$.*

PROOF. Let x be a complement of bc in b, whence $x+bc=b$, $(x, bc)\perp$. Define $b'\equiv a+x\leqq b$. Then

$$b'c = (a + x)c = (a + x)bc = a.$$

Suppose that $(b', c)M$, that is, $(a+x, c)M$. Then $c_1\leqq c$ implies

$$\begin{aligned}(c_1 + b)c &= (c_1 + x + bc)c \\ &= (c_1 + x + a + bc)c \\ &= c_1 + bc + (x + a)c \\ &= c_1 + bc,\end{aligned}$$

contrary to $(b, c)M'$. Hence $(b', c)M'$. The second part follows by putting $a=0$.

THEOREM 4. *If $x\in M_L'$ and $y\leqq x$, then $y\in M_L'$.*

PROOF. Immediate from Lemma 1.

We turn now to a general example of a left complemented lattice. Let Λ be a complemented modular lattice with operations $\oplus$, $\otimes$, and let ∞ be any element of Λ; let L be a subset of Λ with the following properties:

(4) $\mathfrak{a} \equiv [x; x \leqq \infty] \subset L;\ 1 \in L;$

(5) $x \in L,\ x \notin \mathfrak{a},\ y \geqq x$ implies $y \in L;$

(6) $x \in L,\ y \leqq x$ implies the existence of $z \in L$ such that

$$z \oplus y = x, \qquad z \otimes y = 0.$$

A special case is the following. Λ is a projective geometry, and ∞, $h\in\Lambda$, $0<\infty<h<1$, $L'\equiv[x; x\leqq h, x \text{ not } \leqq \infty]$, $L\equiv\Lambda-L'$. Then L obviously satisfies (4) and (5), and (6) holds by virtue of the irreducibility of Λ. If h is a hyperplane, that is, h is a maximal element less than 1, then L is an affine geometry (for example, Λ with h as ideal hyperplane) with the ideal elements of $\mathfrak{a}$ restored.

THEOREM 5. *L is a lattice in which the operations $+$, $\cdot$ are given by*

$$(7) \qquad a + b = a \oplus b, \qquad ab = \begin{cases} a \otimes b & \text{if } a \otimes b \in L \\ a \otimes b \otimes \infty & \text{otherwise.} \end{cases}$$

PROOF. To show that $a \oplus b$ is a least upper bound of a, b in L it suffices to prove that $a, b \in L$ implies $a \oplus b \in L$. If both $a, b \in \mathfrak{a}$, then $a \oplus b \in L$ by (4). Hence suppose $a \notin \mathfrak{a}$; by (5) $a \oplus b \in L$. We shall prove directly that ab as defined in (7) is effective as greatest lower bound of a, b in L. Clearly $ab \leqq a, b$; by (4) $ab \in L$. Let $c \in L$, $c \leqq a, b$. Then $c \leqq a \otimes b$. If $c \notin \mathfrak{a}$, then $a \otimes b \in L$, and $c \leqq ab$ by (7). If $c \in \mathfrak{a}$, then $c \leqq a \otimes b \otimes \infty \leqq ab$.

COROLLARY. *If $a \in \mathfrak{a}$, $b \in L$, then $ab = a \otimes b$.*

LEMMA 2. *If $b, c \in L$, then $(b, c)M$ if and only if $b \otimes c \in L$.*

PROOF. First let $(b, c)M$, and suppose $b \otimes c \notin L$. Let $a \in L$ be a complement of $b \otimes c$ in c, existent by (6). Then

$$(a \oplus b) \otimes c = a \oplus (b \otimes c) = c,$$

whence $(a \oplus b) \otimes c \in L$; thus by (7)

$$a \oplus (b \otimes c) = (a \oplus b) \otimes c = (a + b)c = a + bc = a \oplus (b \otimes c \otimes \infty),$$

and it follows from the theory of modular lattices that $(b \otimes c) \otimes \infty = b \otimes c$. By (4) this contradicts the hypothesis, whence $b \otimes c \in L$. Conversely, let $b \otimes c \in L$, and let $a \leqq c$, $a \in L$. If $a \notin \mathfrak{a}$, then $(a \oplus b) \otimes c \in L$, and by (7) and the modular law in Λ we have

$$(8) \qquad (a + b)c = (a \oplus b) \otimes c = a \oplus (b \otimes c) = a + bc.$$

Suppose $a \in \mathfrak{a}$. If $(a \oplus b) \otimes c \in L$, equalities (8) hold. If $(a \oplus b) \otimes c \notin L$, then

$$(9) \qquad \begin{aligned} (a + b)c &= (a \oplus b) \otimes c \otimes \infty = (a \oplus (b \otimes c)) \otimes \infty \\ &= a \oplus (b \otimes c \otimes \infty) \leqq a + bc \leqq (a + b)c. \end{aligned}$$

By (8) and (9) we have $(b, c)M$.

COROLLARY. *L is M-symmetric.*

THEOREM 6. *The lattice L is left complemented.*

PROOF. Let $a, b \in L$, and let $b_1 \in L$ be a complement of $a \otimes b$ in b, existent by (6). Then

$$a + b_1 = a \oplus (a \otimes b) \oplus b_1 = a \oplus b = a + b;$$
$$a \otimes b_1 = a \otimes b \otimes b_1 = 0 \in \mathfrak{a} \subset L,$$

whence $(a, b_1)M$ by Lemma 2. But $ab_1 = 0$, and it follows from the corollary to Lemma 2 that $(b_1, a)\perp$. Thus b_1 is a (left) complement within b of a in $a + b$.

THEOREM 7. *The set* $\mathfrak{a}$ *is a modular ideal in* L *containing the set* M_L'.

PROOF. It is obvious that $\mathfrak{a}$ is an ideal; that it is modular follows from the corollary to Theorem 5, equations (7) and Lemma 2. Now if $(b, c)M'$, then by Lemma 2 $b \otimes c \notin L$, whence $bc = (b \otimes c) \otimes \infty$, and $bc \in \mathfrak{a}$. Hence $M_L' \subset \mathfrak{a}$.

It should be observed that both possibilities $M_L' = \mathfrak{a}$ and $M_L' \neq \mathfrak{a}$ can occur. In our special example where Λ is a projective geometry and $\Lambda - L$ consists of all subelements x of a hyperplane h with x not $\leqq \infty$, $M_L' = \mathfrak{a}$ if there exists $k \notin L$ with $\infty < k < h$. On the other hand, if no element exists (in Λ) between ∞ and h, then $M_L' \neq \mathfrak{a}$, for then $\infty \notin M_L'$. This example shows also that M_L' need not be an ideal.

ILLINOIS INSTITUTE OF TECHNOLOGY

SUFFICIENT CONDITIONS THAT POLYNOMIALS IN SEVERAL VARIABLES BE POSITIVE

IRWIN E. PERLIN

1. **Introduction.** Let $T(x)$ denote a polynomial in a single real variable x with real coefficients. T. Popoviciu[1] established sufficient conditions that $T(x)$ be positive for all real x. In this paper we shall consider polynomials in several real variables with real coefficients, and establish sufficient conditions that the polynomials be positive for real values of the variables.

2. **Polynomials in two real variables.** In this section we shall develop sufficient conditions that a polynomial in two real variables with real coefficients be positive for all real values of the variables. Let us consider then,

$$T(x, y) = \sum_{i=0}^{2m} \sum_{j=0}^{2n} b_{ij} c_{ij} x^i y^j,$$

where the b_{ij} are positive constants, and the c_{ij} are real numbers. Introducing parameters, we write $T(x, y)$ in the following form

---

Presented to the Society, April 13, 1940; received by the editor June 26, 1941.

[1] T. Popoviciu, *Sur une condition suffisante pour qu'un polynôme soit positif*, Mathematica, vol. 11 (1935), pp. 247–256.

$$
\begin{aligned}
T(x, y) = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\Bigg\{ & \alpha_{ij}c_{2i\,2j}x^{2i}y^{2j}\left[\left(1+\beta_{ij}\frac{c_{2i+1\,2j}}{c_{2i\,2j}}x\right)^2\right. \\
& \left.+\left(1+\gamma_{ij}\frac{c_{2i\,2j+1}}{c_{2i\,2j}}y\right)^2\right] \\
& +\zeta_{ij}\frac{(1/\lambda^2)c_{2i\,2j}c_{2i+2\,2j}-c_{2i+1\,2j}^2}{c_{2i\,2j}}x^{2i+2}y^{2j} \\
& +\eta_{ij}\frac{(1/\lambda^2)c_{2i\,2j}c_{2i\,2j+2}-c_{2i\,2j+1}^2}{c_{2i\,2j}}x^{2i}y^{2j+2}\Bigg\} \\
& +\sum_{j=0}^{n-1}\Bigg\{2\alpha_{mj}c_{2m\,2j}x^{2m}y^{2j}\left(1+\gamma_{mj}\frac{c_{2m\,2j+1}}{2c_{2m\,2j}}y\right)^2 \\
& +\eta_{mj}\frac{(1/\lambda^2)c_{2m\,2j}c_{2m\,2j+2}-(1/2)c_{2m\,2j+1}^2}{c_{2m\,2j}}x^{2m}y^{2j+2}\Bigg\} \\
& +\sum_{i=0}^{m-1}\Bigg\{2\alpha_{in}c_{2i\,2n}x^{2i}y^{2n}\left(1+\beta_{in}\frac{c_{2i+1\,2n}}{2c_{2i\,2n}}x\right)^2 \\
& +\zeta_{in}\frac{(1/\lambda^2)c_{2i\,2n}c_{2i+2\,2n}-(1/2)c_{2i+1\,2n}^2}{c_{2i\,2n}}x^{2i+2}y^{2n}\Bigg\} \\
& +\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}b_{2i+1\,2j+1}c_{2i+1\,2j+1}x^{2i+1}y^{2j+1}+2\alpha_{mn}c_{2m\,2n}x^{2m}y^{2n}.
\end{aligned}
$$

By comparing coefficients, we find

$$
\begin{aligned}
2\alpha_{00} &= b_{00}, \\
2\alpha_{ij}\beta_{ij} &= b_{2i+1\,2j}, \qquad \zeta_{ij} = \beta_{ij}^2\alpha_{ij}, \\
& \qquad i = 0, 1, \cdots, m-1;\ j = 0, 1, \cdots, n, \\
2\alpha_{ij}\gamma_{ij} &= b_{2i\,2j+1}, \qquad \eta_{ij} = \gamma_{ij}^2\alpha_{ij}, \\
& \qquad i = 0, 1, \cdots, m;\ j = 0, 1, \cdots, n-1,
\end{aligned}
$$

$$
\frac{1}{\lambda^2}\zeta_{i-1\,0}+2\alpha_{i0} = b_{2i\,0}, \qquad i = 1, 2, \cdots, m,
$$

$$
\frac{1}{\lambda^2}\eta_{0\,j-1}+2\alpha_{0j} = b_{0\,2j}, \qquad i = 1, 2, \cdots, n,
$$

$$
\frac{1}{\lambda^2}\zeta_{i-1\,j}+\frac{1}{\lambda^2}\eta_{i\,j-1}+2\alpha_{ij} = b_{2i\,2j},
$$

$$
i = 1, 2, \cdots, m;\ j = 1, 2, \cdots, n.
$$

We define $\zeta_{-1j}=\eta_{i-1}=0$ $(i=0, 1, \cdots, m; j=0, 1, \cdots, n)$. The last three equations can be written

$$\frac{1}{\lambda^2}\zeta_{i-1\ j}+\frac{1}{\lambda^2}\eta_{i\ j-1}+2\alpha_{ij}=b_{2i\ 2j},$$

$$i=0, 1, \cdots, m; j=0, 1, \cdots, n.$$

The parameters α_{ij} are determined by the recursion relations

$$\alpha_{ij}=\frac{4\lambda^2 b_{2i\ 2j}\alpha_{i-1\ j}\alpha_{i\ j-1}-b_{2i-1\ 2j}^2\alpha_{i\ j-1}-b_{2i\ 2j-1}^2\alpha_{i-1\ j}}{8\lambda^2\alpha_{i-1\ j}\alpha_{i\ j-1}},$$

where we have defined $b_{-1j}=b_{i-1}=0$ and $\alpha_{i-1}=\alpha_{-1j}=1$ $(i=0, 1, \cdots, m; j=0, 1, \cdots, n)$. Let us write

$$\alpha_{ij}=\frac{P_{ij}(\lambda)}{2\lambda Q_{ij}(\lambda)},$$

where $P_{ij}(\lambda)$ and $Q_{ij}(\lambda)$ are polynomials in λ. The polynomials $P_{ij}(\lambda)$ and $Q_{ij}(\lambda)$ satisfy the recursion relations

$$\begin{aligned}
P_{00}(\lambda) &= b_{00}\lambda, \qquad Q_{00}(\lambda)=1,\\
P_{ij}(\lambda) &= \lambda b_{2i\ 2j}Q_{ij}(\lambda)-\tfrac{1}{2}b_{2i-1\ 2j}^2 P_{i\ j-1}(\lambda)Q_{i-1\ j}(\lambda)\\
&\quad -\tfrac{1}{2}b_{2i\ 2j-1}^2 P_{i-1\ j}(\lambda)Q_{i\ j-1}(\lambda),\\
Q_{ij}(\lambda) &= P_{i-1\ j}(\lambda)P_{i\ j-1}(\lambda),
\end{aligned}$$

where we define $P_{-1j}(\lambda)=P_{i-1}(\lambda)=Q_{-1j}(\lambda)=Q_{i-1}(\lambda)=1$ $(i=0, 1, \cdots, m; j=0, 1, \cdots, n)$. Let λ_{ij} be the greatest positive zero of $P_{ij}(\lambda)$. Then we establish the following lemma.

LEMMA 1. *$\bar{\lambda}_{ij}$ is greater than or equal to the greater of $\bar{\lambda}_{i-1\ j}$ and $\bar{\lambda}_{i\ j-1}$.*

We proceed to prove this lemma by induction. Obviously $\bar{\lambda}_{10}\geqq\bar{\lambda}_{00}$ and $\bar{\lambda}_{01}\geqq\bar{\lambda}_{00}$. Since the degree of $P_{i-1\ j}(\lambda)$ is greater than that of $P_{i-1\ j-1}(\lambda)P_{i-2\ j}(\lambda)$ and the degree of $P_{i\ j-1}(\lambda)$ is greater than that of $P_{i-1\ j-1}(\lambda)P_{i\ j-2}(\lambda)$, it follows that the degree of $P_{ij}(\lambda)$ is the same as that of $\lambda b_{2i\ 2j}P_{i-1\ j}(\lambda)P_{i\ j-1}(\lambda)$. We see that the coefficient of the highest power of λ in $P_{ij}(\lambda)$ is positive. Let τ equal the greater of $\bar{\lambda}_{i-1\ j}$ and $\bar{\lambda}_{i\ j-1}$. Then $P_{ij}(\tau)\leqq 0$. Hence, $\bar{\lambda}_{ij}$ is greater than or equal to the greater of $\bar{\lambda}_{i-1\ j}$ and $\bar{\lambda}_{i\ j-1}$.

THEOREM 1. *Let r be a real constant. If $r>\bar{\lambda}_{mn}$, and*

$$c_{00}>0,$$

$$\frac{1}{r^2}c_{2i\,2j}c_{2i+2\,2j} - c^2_{2i+1\,2j} > 0,$$
$$i = 0, 1, \cdots, m-1; j = 0, 1, \cdots, n-1,$$

$$\frac{1}{r^2}c_{2i\,2n}c_{2i+2\,2n} - \tfrac{1}{2}c^2_{2i+1\,2n} > 0, \qquad i = 0, 1, \cdots, m-1,$$

$$\frac{1}{r^2}c_{2i\,2j}c_{2i\,2j+2} - c^2_{2i\,2j+1} > 0$$
$$i = 0, 1, \cdots, m-1; j = 0, 1, \cdots, n-1,$$

$$\frac{1}{r^2}c_{2m\,2j}c_{2m\,2j+2} - \tfrac{1}{2}c^2_{2m\,2j+1} > 0, \qquad j = 0, 1, \cdots n, -1,$$

$$c_{2i+1\,2j+1} = 0, i = 0, 1, \cdots, \quad m-1; j = 0, 1 \cdots, n-1.$$

then $T(x, y) > 0$ for all real values of x and y.

By the preceding lemma $P_{ij}(r) > 0$ $(i = 0, 1, \cdots, m; j = 0, 1, \cdots, n)$. Hence $\alpha_{ij} > 0$ $(i = 0, 1, \cdots, m; j = 0, 1, \cdots, n)$, $\zeta_{ij} > 0$ $(i = 0, 1, \cdots, m-1; j = 0, 1, \cdots, n)$, and $\eta_{ij} > 0$ $(i = 0, 1, \cdots, m; j = 0, 1, \cdots, n-1)$. It follows that $T(x, y) > 0$ for all real x and y.

3. **Applications.** In this section we shall study the case where $b_{ij} = 1$ $(i = 0, 1, \cdots, 2m; j = 0, 1, \cdots, 2n)$, and deduce a sufficient condition that the polynomial

$$L(x, y) = \sum_{i=0}^{2m}\sum_{j=0}^{2n} c_{ij}x^i y^j$$

be positive for all real values of x and y. For this case, the polynomials $P_{ij}(\lambda)$ satisfy the recursion relations

$$P_{00}(\lambda) = \lambda,$$
$$P_{i0}(\lambda) = \lambda P_{i-1\,0}(\lambda) - \tfrac{1}{2}P_{i-2\,0}(\lambda), \qquad i = 1, 2, \cdots, m,$$
$$P_{0j}(\lambda) = \lambda P_{0\,j-1}(\lambda) - \tfrac{1}{2}P_{0\,j-2}(\lambda), \qquad j = 1, 2, \cdots, n,$$
$$P_{ij}(\lambda) = \lambda P_{i-1\,j}(\lambda)P_{i\,j-1}(\lambda) - \tfrac{1}{2}P_{i\,j-1}(\lambda)P_{i-1\,j-1}(\lambda)P_{i-2\,j}(\lambda)$$
$$- \tfrac{1}{2}P_{i-1\,j}(\lambda)P_{i-1\,j-1}(\lambda)P_{i\,j-2}(\lambda),$$
$$i = 1, 2, \cdots, m; j = 1, 2, \cdots, n,$$

where we define $P_{-1\,j}(\lambda) = P_{i-1}(\lambda) = 1$ $(i = 0, 1, \cdots, m; j = 0, 1, \cdots, n)$.

LEMMA 2. $\bar{\lambda}_{ij} < 2, \quad i = 0, 1, \cdots, m; j = 0, 1, \cdots, n.$

We shall prove this lemma by showing that

$$P_{ij}(\lambda) \geqq P_{i-1\,j}(\lambda) \cdot P_{i\,j-1}(\lambda) > 0, \qquad \lambda \geqq 2.$$

We establish this result by induction. It is seen that the above is true for $i+j=0$ and 1. Now

$$P_{i0}(\lambda) = \lambda P_{i-1\,0}(\lambda) - \tfrac{1}{2}P_{i-2\,0}(\lambda),$$
$$P_{i0}(\lambda) \geqq (\lambda - \tfrac{1}{2})P_{i-1\,0}(\lambda) > 0, \qquad \lambda \geqq 2,$$
$$P_{i0}(\lambda) \geqq P_{i-1\,0}(\lambda) > 0, \qquad \lambda \geqq 2.$$

And since $P_{0j}(\lambda) = P_{j0}(\lambda)$ it follows that

$$P_{0j}(\lambda) \geqq P_{0\,j-1}(\lambda) > 0, \qquad \lambda \geqq 2.$$

Now

$$P_{ij}(\lambda) = \lambda P_{i-1\,j}(\lambda)P_{i\,j-1}(\lambda) - \tfrac{1}{2}P_{i\,j-1}(\lambda)P_{i-1\,j-1}(\lambda)P_{i-2\,j}(\lambda) - \tfrac{1}{2}P_{i-1\,j}(\lambda)P_{i-1\,j-1}(\lambda)P_{i\,j-2}(\lambda),$$
$$P_{ij}(\lambda) \geqq (\lambda - 1)P_{i-1\,j}(\lambda)P_{i\,j-1}(\lambda) > 0, \qquad \lambda \geqq 2,$$
$$P_{ij}(\lambda) \geqq P_{i-1\,j}(\lambda)P_{i\,j-1}(\lambda) > 0, \qquad \lambda \geqq 2.$$

Hence $\bar{\lambda}_{ij} < 2$ $(i=0, 1, \cdots, m; j=0, 1, \cdots, n)$. From Theorem 1 and Lemma 2 we have immediately the following result.

THEOREM 2. *If* $c_{00} > 0$,

$$c_{2i\,2j}c_{2i+2\,2j} - 4c^{2}_{2i+1\,2j} > 0, \qquad i = 0, 1, \cdots, m-1; j = 0, 1, \cdots, n-1,$$
$$c_{2i\,2n}c_{2i+2\,2n} - 2c^{2}_{2i+1\,2n} > 0, \qquad i = 0, 1, \cdots, m-1,$$
$$c_{2i\,2j}c_{2i\,2j+2} - 4c^{2}_{2i\,2j+1} > 0, \qquad i = 0, 1, \cdots, m-1; j = 0, 1, \cdots, n-1,$$
$$c_{2m\,2j}c_{2m\,2j+2} - 2c^{2}_{2m\,2j+1} > 0, \qquad j = 0, 1, \cdots, n-1,$$
$$c_{2i+1\,2j+1} = 0, \qquad i = 0, 1, \cdots, m-1; j = 0, 1, \cdots, n-1,$$

then $L(x, y) > 0$ *for all real values of* x *and* y.

This theorem is a generalization of the theorem of E. B. Van Vleck[2] for the case of a polynomial in a single real variable x.

4. **Polynomials in several real variables.** Let

$$(1) \qquad T(x_1, x_2, \cdots, x_n) = \sum_{p=0}^{2u}\sum_{q=0}^{2v}\cdots\sum_{r=0}^{2w} b_{pq\cdots r}c_{pq\cdots r}x_1^{p}x_2^{q}\cdots x_n^{r},$$

[2] E. B. Van Vleck, *A sufficient condition for the maximum number of imaginary roots of an equation of the nth degree*, Annals of Mathematics (2), vol. 4 (1902–1903), p. 191.

where the $b_{pq\cdots r}$ are positive constants, and the $c_{pq\cdots r}$ are real numbers. Let A denote the class of all the distinct permutations $ij\cdots k$ where i ranges from 0 to u, j ranges from 0 to v, $\cdots$, and k ranges from 0 to w. We define the following $n+1$ functions over the class A

$$I_{ij\cdots k} = \begin{matrix} 1, & i \neq u \\ 0, & i = u \end{matrix}, \quad J_{ij\cdots k} = \begin{matrix} 1, & j \neq v \\ 0, & j = v \end{matrix}, \quad \cdots, \quad K_{ij\cdots k} = \begin{matrix} 1, & k \neq w \\ 0, & k = w \end{matrix},$$

$$S_{ij\cdots k} = \frac{n}{n - d_{ij\cdots k}}, \qquad ij\cdots k \neq uv\cdots w,$$

$$S_{uv\cdots w} = n,$$

where $d_{ij\cdots k}$ represents the number of the indices $i, j, \cdots, k$ which are equal to $u, v, \cdots, w$, respectively. Introducing parameters we rewrite the polynomial (1) as

$$T(x_1, x_2, \cdots, x_n) = \sum_A \Bigg[S_{ij\cdots k}\alpha_{ij\cdots k}c_{2i\,2j\cdots 2k}x_1^{2i}x_2^{2j}\cdots x_n^{2k}$$

$$\Bigg\{ I_{ij\cdots k}\left(1 + \beta_{ij\cdots k}\frac{c_{2i+1\,2j\cdots 2k}}{S_{ij\cdots k}c_{2i\,2j\cdots 2k}}x_1\right)^2$$

$$+ J_{ij\cdots k}\left(1 + \gamma_{ij\cdots k}\frac{c_{2i\,2j+1\cdots 2k}}{S_{ij\cdots k}c_{2i\,2j\cdots 2k}}x_2\right)^2 + \cdots$$

$$+ K_{ij\cdots k}\left(1 + \delta_{ij\cdots k}\frac{c_{2i\,2j\cdots 2k+1}}{S_{ij\cdots k}c_{2i\,2j\cdots 2k}}x_n\right)^2 \Bigg\} + I_{ij\cdots k}\zeta_{ij\cdots k}$$

$$\cdot\frac{(1/\lambda^2)c_{2i\,2j\cdots 2k}c_{2i+2\,2j\cdots 2k} - c_{2i+1\,2j\cdots 2k}^2/S_{ij\cdots k}}{c_{2i\,2j\cdots 2k}}x_1^{2i+2}x_2^{2j}\cdots x_n^{2k}$$

$$+ J_{ij\cdots k}\eta_{ij\cdots k}\frac{(1/\lambda^2)c_{2i\,2j\cdots 2k}c_{2i\,2j+2\cdots 2k} - c_{2i\,2j+1\cdots 2k}^2/S_{ij\cdots k}}{c_{2i\,2j\cdots 2k}}$$

$$\cdots x_1^{2i}\cdots x_2^{2j+2}\cdots x_n^{2k} + \cdots + K_{ij\cdots k}\mu_{ij\cdots k}$$

$$\cdot\frac{(1/\lambda^2)c_{2i\,c_{2j}\cdots 2k}c_{2i\,2j\cdots 2k+2} - c_{2i\,2j\cdots 2k+1}^2/S_{ij\cdots k}}{c_{2i\,2j\cdots 2k}}x_1^{2i}x_2^{2j}\cdots x_n^{2k+2}\Bigg]$$

$$+ \sum_{p=0}^{u-1}\sum_{q=0}^{v-1}\cdots\sum_{r=0}^{w-1} b_{2p+1\,2q+1\cdots 2r+1}c_{2p+1\,2q+1\cdots 2r+1}x_1^{2p+1}x_2^{2q+1}\cdots x_n^{2r+1},$$

where $\sum_A$ means that the summation shall extend over all permutations $ij\cdots k\in A$. By comparing coefficients we obtain

$$
\begin{aligned}
n\alpha_{00\cdots0} &= b_{00\cdots0},\\
2\alpha_{ij\cdots k}\beta_{ij\cdots k} &= b_{2i+1\,2j\cdots2k},\\
2\alpha_{ij\cdots k}\gamma_{ij\cdots k} &= b_{2i\,2j+1\cdots2k},\\
&\cdots\cdots\cdots\cdots,\\
2\alpha_{ij\cdots k}\delta_{ij\cdots k} &= b_{2i\,2j\cdots2k+1},\\
\zeta_{ij\cdots k} &= \alpha_{ij\cdots k}\beta^2_{ij\cdots k},\\
\eta_{ij\cdots k} &= \alpha_{ij\cdots k}\gamma^2_{ij\cdots k},\\
&\cdots\cdots\cdots\cdots,\\
\mu_{ij\cdots k} &= \alpha_{ij\cdots k}\delta^2_{ij\cdots k},\\
n\alpha_{ij\cdots k}+\frac{1}{\lambda^2}(\zeta_{i-1\,j\cdots k}+\eta_{i\,j-1\cdots k}+\cdots+\mu_{ij\cdots k-1}) &= b_{2i\,2j\cdots2k},
\end{aligned}
$$

where we define $\zeta_{ij\cdots k}=\eta_{ij\cdots k}=\cdots=\mu_{ij\cdots k}=0$, $\alpha_{ij\cdots k}=1$, $ij\cdots k\notin A$; $b_{pq\cdots r}=0$ if $p, q, \cdots, r$ are not in the ranges 0 to $2u$, 0 to $2v$, $\cdots$, 0 to $2w$, respectively. The parameters $\alpha_{ij\cdots k}$ are determined by the recursion relations

$$
\begin{aligned}
n\alpha_{00\cdots0} &= b_{00\cdots0},\\
4n\lambda^2\alpha_{ij\cdots k} &= 4\lambda^2 b_{2i\,2j\cdots2k}-\left(\frac{b^2_{2i-1\,2j\cdots2k}}{\alpha_{i-1\,j\cdots k}}+\frac{b^2_{2i\,2j-1\cdots2k}}{\alpha_{i\,j-1\cdots k}}+\cdots\right.\\
&\qquad\left.+\frac{b^2_{2i\,2j\cdots2k-1}}{\alpha_{ij\cdots k-1}}\right).
\end{aligned}
$$

We write $\alpha_{ij\cdots k}=P_{ij\cdots k}(\lambda)/n\lambda Q_{ij\cdots k}(\lambda)$, where $P_{ij\cdots k}(\lambda)$ and $Q_{ij\cdots k}(\lambda)$ are polynomials in λ. The polynomials $P_{ij\cdots k}(\lambda)$ and $Q_{ij\cdots k}(\lambda)$ satisfy the recursion relations

$$
\begin{aligned}
P_{00\cdots0}(\lambda) &= b_{00\cdots0}\lambda, \qquad Q_{00\cdots0}(\lambda)=1,\\
P_{ij\cdots k}(\lambda) &= Q_{ij\cdots k}(\lambda)\left\{\lambda b_{2i\,2j\cdots2k}-\frac{n}{4}\left[\frac{b^2_{2i-1\,2j\cdots2k}Q_{i-1\,j\cdots k}(\lambda)}{P_{i-1\,j\cdots k}(\lambda)}\right.\right.\\
&\qquad+\frac{b^2_{2i\,2j-1\cdots2k}Q_{i\,j-1\cdots k}(\lambda)}{P_{i\,j-1\cdots k}(\lambda)}+\cdots\\
&\qquad\left.\left.+\frac{b^2_{2i\,2j\cdots2k-1}Q_{ij\cdots k-1}(\lambda)}{P_{ij\cdots k-1}(\lambda)}\right]\right\},\\
Q_{ij\cdots k}(\lambda) &= P_{i-1\,j\cdots k}(\lambda)P_{i\,j-1\cdots k}(\lambda)\cdots P_{ij\cdots k-1}(\lambda),
\end{aligned}
$$

where we define $P_{ij\cdots k}(\lambda)=Q_{ij\cdots k}(\lambda)=1$ for $ij\cdots k\notin A$. Let $\bar{\lambda}_{ij\cdots k}$ be the greatest positive zero of $P_{ij\cdots k}(\lambda)$. Then we can establish the following lemma.

LEMMA 3. *$\bar{\lambda}_{ij\cdots k}$ is greater than or equal to the greater of $\bar{\lambda}_{i-1\ j\cdots k}$, $\bar{\lambda}_{i\ j-1\cdots k}$, $\cdots$, $\bar{\lambda}_{ij\cdots k-1}$.*

The proof of this lemma is similar to that given for Lemma 1.

THEOREM 3. *Let r be a real constant. If $r\geqq\bar{\lambda}_{uv\cdots w}$, and*

$$c_{00\cdots 0}>0,$$

$$\frac{1}{r^2}c_{2i\ 2j\cdots 2k}c_{2i+2\ 2j\cdots 2k}-\frac{c^2_{2i+1\ 2j\cdots 2k}}{S_{ij\cdots k}}>0,$$

$$\frac{1}{r^2}c_{2i\ 2j\cdots 2k}c_{2i\ 2j+2\cdots 2k}-\frac{c^2_{2i\ 2j+1\cdots 2k}}{S_{ij\cdots k}}>0,$$

$$\frac{1}{r^2}c_{2i\ 2j\cdots 2k}c_{2i\ 2j\cdots 2k+2}-\frac{c^2_{2i\ 2j\cdots 2k+1}}{S_{ij\cdots k}}>0,$$

$$c_{2i+1\ 2j+1\cdots 2k+1}=0,$$

then

$$T(x_1, x_2, \cdots, x_n)>0$$

for all real values of $x_1, x_2, \cdots, x_n$.

This theorem follows from the preceding lemma in the same manner that Theorem 1 follows from Lemma 1.

If we take the coefficients

$$b_{pq\cdots r}=1,$$

we can deduce a result generalizing Theorem 2. We consider the polynomial

$$L(x_1, x_2, \cdots, x_n)=\sum_{p=0}^{2u}\sum_{q=0}^{2v}\cdots\sum_{r=0}^{2w}c_{pq\cdots r}x_1^p x_2^q\cdots x_n^r.$$

We define over the class A the following n functions

$$f_{ij\cdots k}=\begin{matrix}0,\ i=0\\ 1,\ i\neq 0\end{matrix},\quad g_{ij\cdots k}=\begin{matrix}0,\ j=0\\ 1,\ j\neq 0\end{matrix},\quad\cdots,\quad h_{ij\cdots k}=\begin{matrix}0,\ k=0\\ 1,\ k\neq 0\end{matrix}.$$

The recursion relations that the polynomials $P_{ij\cdots k}(\lambda)$ satisfy in this case are

$$P_{00\cdots0}(\lambda) = \lambda,$$

$$P_{ij\cdots k}(\lambda) = Q_{ij\cdots k}(\lambda)\left(\lambda - \frac{n}{4}\left[f_{ij\cdots k}\frac{Q_{i-1\,j\cdots k}(\lambda)}{P_{i-1\,j\cdots k}(\lambda)} + g_{ij\cdots k}\frac{Q_{ij-1\cdots k}(\lambda)}{P_{ij-1\cdots k}(\lambda)} + \cdots + h_{ij\cdots k}\frac{Q_{ij\cdots k-1}(\lambda)}{P_{ij\cdots k-1}(\lambda)}\right]\right),$$

$$Q_{ij\cdots k}(\lambda) = P_{i-1j\cdots k}(\lambda)P_{ij-1\cdots k}(\lambda)\cdots P_{ij\cdots k-1}(\lambda),$$

where we have defined $P_{ij\cdots k}(\lambda) = Q_{ij\cdots k}(\lambda) = 1$ for $ij\cdots k \notin A$.

LEMMA 4. $\bar{\lambda}_{ij\cdots k} < n^2/4+1$.

The proof of this lemma is similar to that given for Lemma 2.

THEOREM 4. If $c_{00\cdots0} > 0$, *and*

$$\frac{16}{(n^2+4)^2}c_{2i\,2j\cdots2k}c_{2i+2\,2j\cdots2k} - \frac{c^2_{2i+1\,2j\cdots2k}}{S_{ij\cdots k}} > 0,$$

$$\frac{16}{(n^2+4)^2}c_{2i\,2j\cdots2k}c_{2i\,2j+2\cdots2k} - \frac{c^2_{2i\,2j+1\cdots2k}}{S_{ij\cdots k}} > 0,$$

$$\frac{16}{(n^2+4)^2}c_{2i\,2j\cdots2k}c_{2i\,2j\cdots2k+2} - \frac{c^2_{2i\,2j\cdots2k+1}}{S_{ij\cdots k}} > 0,$$

$$c_{2i+1\,2j+1\cdots2k+1} = 0,$$

then $L(x_1, x_2, \cdots, x_n) > 0$ *for all real values of* $x_1, x_2, \cdots, x_n$.

ILLINOIS INSTITUTE OF TECHNOLOGY

ON THE MAPPING OF n QUADRATIC FORMS

LLOYD L. DINES

If $Q_1(z), Q_2(z), \cdots, Q_n(z)$ are quadratic forms in the real variables $z^1, z^2, \cdots, z^m$ with real coefficients, the question arises as to the conditions under which there exists a linear combination

$$\lambda_1 Q_1(z) + \lambda_2 Q_2(z) + \cdots + \lambda_n Q_n(z)$$

which is positive definite. A number of recent papers have considered this question.

For the case $n=2$ a satisfactory answer was obtained by Paul Finsler,[1] and independently by a group of interested persons at the University of Chicago.[2]

For any finite n, Finsler obtained sufficient conditions under the restriction that the number of independent variables does not exceed four. The conditions are quite involved, and are in terms of a certain type of algebraic manifold which Finsler designates "Freigebilde" and of which he had made an elaborate study in an earlier paper.

For any finite n and any finite number of independent variables Hestenes and McShane, in a joint paper,[3] obtained sufficient conditions. They are obviously not necessary, and though they seem exactly suited to the application which the authors desired to make, their lack of symmetry perhaps leaves something to be desired.

In a recent paper[4] the present author called attention to the suitability of the theory of convexity as a means for studying this type of question, and treated the case of two quadratic forms in m variables from this point of view. The purpose of the present paper is to make a similar study of the general case of n quadratic forms in m variables.

1. **The map $\mathfrak{M}$.** The n quadratic forms $Q_1(z), Q_2(z), \cdots, Q_n(z)$ may be thought of as mapping the m-dimensional space $\mathfrak{Z}_m$ of points $z=(z^1, z^2, \cdots, z^m)$ onto an n-dimensional space $\mathfrak{X}_n$ of points

Presented to the Society, December 31, 1941; received by the editors September 5, 1941.

[1] *Über das Vorkommen definiter und semidefiniter Formen in Scharen quadratischer Formen*, Commentarii Mathematici Helvetici, vol. 9 (1937), pp. 188–192.

[2] From this group two different proofs of the essential theorem appeared: one by A. A. Albert, this Bulletin, vol. 44 (1938), pp. 250–253; and one by W. T. Reid, ibid., pp. 437–440.

[3] *A theorem on quadratic forms and its application in the calculus of variations*, Transactions of this Society, vol. 47 (1940), pp. 501–512.

[4] *On the mapping of quadratic forms*, this Bulletin, vol. 47 (1941), pp. 494–498.

$x=(x^1, x^2, \cdots, x^n)$. The map $\mathfrak{M}$ consists of the set of points x defined by

$$x = (Q_1(z), Q_2(z), \cdots, Q_n(z)), \qquad z \text{ on } \mathfrak{Z}_m,$$

a formula which may be condensed to

$$\mathfrak{M}: \quad x = Q(z), \qquad z \text{ on } \mathfrak{Z}_m.$$

In view of the homogeneity property

$$Q(tz) = t^2 Q(z) \tag{1}$$

the map consists of half-lines emanating from the origin $x=(0)$. In the particular case $n=2$ it is convex, as was shown in the earlier paper. For $n>2$ it is not necessarily convex. For example, the map of three quadratic forms in two variables lies on a conical surface. It is not necessarily closed, but it may be shown to be closed if the forms $Q_i(z)$ have no common zero except $z=(0)$. However, more useful for our present purpose than the map $\mathfrak{M}$ itself is a certain subset of it which we now define.

2. **The map $\mathfrak{M}_1$.** By $\mathfrak{M}_1$ we shall denote the subset consisting of those points of $\mathfrak{M}$ which correspond to points z on the unit $(m-1)$-sphere in $\mathfrak{Z}_m$. The formula for the points of $\mathfrak{M}_1$ is then

$$\mathfrak{M}_1: \quad x = Q(z), \qquad \|z\| = 1.$$

The particular usefulness of the map $\mathfrak{M}_1$ is due to the facts that it is *bounded* and *closed*, and that it contains the origin $x=(0)$ only in exceptional cases. That it is bounded follows immediately from the continuity of $Q(z)$ on the $(m-1)$-sphere. That it is closed may be seen as follows.

Suppose $\{x_j\}$ is a sequence of points in $\mathfrak{M}_1$ defined by

$$x_j = Q(z_j), \qquad \|z_j\| = 1, \tag{2}$$

and suppose there is in the space $\mathfrak{X}_n$ a point $\bar{x}$ such that

$$\bar{x} = \lim_{j\to\infty} x_j. \tag{3}$$

We will prove that $\bar{x}$ belongs to $\mathfrak{M}_1$.

The sequence of points $\{z_j\}$ on the $(m-1)$-sphere $\|z\|=1$ has an accumulation point $\bar{z}$, which must itself be on the $(m-1)$-sphere (that is, $\|\bar{z}\|=1$), since otherwise it would be a definite distance from it. And from the sequence $\{z_j\}$ there can be chosen a subsequence $\{z_{j_k}\}$ such that

$$\lim_{k\to\infty} z_{j_k} = \bar{z}. \tag{4}$$

Then from (2), (3), (4), and the continuity of $Q(z)$ it follows that $\bar{x}=Q(\bar{z})$, and hence $\bar{x}$ belongs to $\mathfrak{M}_1$.

3. **The convex extension of $\mathfrak{M}_1$.** The convex extension of a set of points may be defined as the smallest convex set which contains it, or (equivalently) as consisting of those points which can be the centroids of positive mass distribution (of total mass unity) at suitably chosen points of the given set. According to the latter definition, $C(\mathfrak{M}_1)$, the convex extension of $\mathfrak{M}_1$, consists of the points represented by

$$C(\mathfrak{M}_1): \quad x = \sum_{j=1}^{r} m_j Q(z_j)$$

where

$$\|z_j\| = 1,\ m_j > 0, \quad \textit{and} \quad \sum_{j=1}^{r} m_j = 1. \tag{5}$$

It may also be remarked that whenever a representation (5) exists, there exists an equivalent one in which the number r of terms in the summation does not exceed $n+1$.

4. **On the existence of a definite $\sum\lambda_i Q_i(z)$.** It is well known that through each point exterior to the convex extension of a bounded and closed set of points there passes a bounding plane[5] (Schranke) for the set, while through no point of the convex extension does there pass such a plane. Hence if the origin $x=(0)$ does not belong to $C(\mathfrak{M}_1)$, there is a plane $\sum_{i=1}^{n}\lambda_i x^i=0$ such that

$$\sum_{i=1}^{n} \lambda_i Q_i(z) > 0 \quad \textit{whenever} \quad \|z\| = 1, \tag{6}$$

while if $x=(0)$ does belong to $C(\mathfrak{M}_1)$ there is no such plane. And in view of the homogeneity relation (1), the validity of (6) is obviously equivalent to the validity of the same relation with z restricted only by $z\neq(0)$.

The condition that $x=(0)$ shall belong to $C(\mathfrak{M}_1)$ is that there shall exist valid relations

$$\sum_{j=1}^{r} m_j Q_i(z_j) = 0, \qquad i = 1, 2, \cdots, n, \tag{7}$$

[5] For simplicity we use the term "plane" to designate the locus of a linear equation in the x-coordinates, regardless of the dimensions of the space $\mathfrak{X}_n$.

where the z_j and m_j are restricted as in (5). And again in view of the homogeneity property (1) and the homogeneity of (7) in the m_j, the only essential restrictions are $z_j \neq (0)$ and $m_j > 0$. We have then the following theorem:

THEOREM 1. *A necessary and sufficient condition that there exist a linear combination* $\sum \lambda_i Q_i(z)$ *such that*

$$\sum_{i=1}^{n} \lambda_i Q_i(z) > 0 \quad \textit{when} \quad z \neq (0)$$

is that there exist in $\mathfrak{Z}_m$ *no set of points* $z_j \neq (0)$, $(j = 1, 2, \cdots, r)$ *such that*

$$\sum_{j=1}^{r} m_j Q_i(z_j) = 0, \qquad i = 1, 2, \cdots, n, \tag{8}$$

the coefficients m_j *being positive.*

5. **On the existence of a semi-definite** $\sum \lambda_i Q_i(z)$. We have seen that when $x = (0)$ is exterior to $C(\mathfrak{M}_1)$ there exist definite linear combinations $\sum \lambda_i Q_i(z)$. It is easily seen that under these circumstances there also exist *semi*-definite linear combinations. We seek here however the more critical conditions under which there exists a linear combination which is semi-definite but none which is definite. This is the case when $x = (0)$ is a *boundary* point of $C(\mathfrak{M}_1)$. For in that case there passes through $x = (0)$ a *supporting* plane (Stützebene) $\sum \lambda_i x^i = 0$ for $\mathfrak{M}_1$, such that

$$\sum_{i=1}^{n} \lambda_i Q_i(z) \geqq 0, \qquad z \textit{ on } \mathfrak{Z}_m, \tag{9}$$

the restriction $\|z\| = 1$ being removable in view of the homogeneity property (1). The "$=$" sign in (9) is required for at least one point $z \neq (0)$, and hence the linear combination is truly semi-definite unless the $Q_i(z)$ are linearly dependent. We may now state this theorem:

THEOREM 2. *If the quadratic forms* $Q_i(z)$ *are linearly independent, necessary and sufficient conditions that they admit a linear combination which is semi-definite but none which is definite are*: (a) *that there exist in* $\mathfrak{Z}_m$ *a set of points* $z_j \neq (0)$, $(j = 1, 2, \cdots, r)$ *and associated positive constants* m_j *such that*

$$\sum_{j=1}^{r} m_j Q(z_j) = 0,$$

and (b) *that there exist a set of real constants* $a=(a^1, a^2, \cdots, a^n)$ *not representable in the form*

$$a = \sum_{j=1}^{r} m_j^i Q(z_j^i), \tag{10}$$

each m_j^i *being positive and each* $z_j^i \neq (0)$.

We have already seen that condition (a) is the condition that $x=(0)$ belong to $C(\mathfrak{M}_1)$. Condition (b) is necessary and sufficient to assure that it be a *boundary* point.

It is sufficient, for if some point a of $\mathfrak{X}_n$ is not representable in form (10), then no point on the half-line $x=at$, $(t>0)$, can belong to $C(\mathfrak{M}_1)$, and the origin $x=(0)$ can be approached by a sequence of exterior points on this half-line.

It is necessary, for in its absence every point a of the space $\mathfrak{X}_n$ is representable in form (10), and as a result some point on every half-line $x=at$, $(t>0)$, belongs to $C(\mathfrak{M}_1)$. And since the origin $x=(0)$ itself belongs to $C(\mathfrak{M}_1)$, it follows that there is a hypercube with this origin at its center and all of its vertices belonging to $C(\mathfrak{M}_1)$. The origin would then be an inner point of $C(\mathfrak{M}_1)$.

6. **Generalization.** Of the various properties of quadratic forms, only their continuity and their quadratic homogeneity were used in the above discussion. Indeed it remains valid if: (1) the m-dimensional space $\mathfrak{Z}_m$ is replaced by any normed linear space $\mathfrak{Z}$ in which the points on the unit hypersphere $\|z\|=1$ form a compact subspace; and (2) the n functions $Q_i(z)$ are real-valued functions on $\mathfrak{Z}$, continuous on the hypersphere $\|z\|=1$, and having the property that for real t, $Q_i(tz) = p(t)Q_i(z)$, where $p(t)$ is a non-negative real-valued function which vanishes when and only when $t=0$ and which has a real-valued inverse $t(p)$, not necessarily unique, but defined for all positive p.

CARNEGIE INSTITUTE OF TECHNOLOGY

MEASURE AND OTHER PROPERTIES OF A HAMEL BASIS

F. B. JONES

A Hamel basis[1] is a set $a, b, c, \cdots$ of real numbers such that if x is any real number whatsoever then x may be expressed uniquely in the form $\alpha a+\beta b+\gamma c+\cdots$ where $\alpha, \beta, \gamma, \cdots$ are rational numbers of which only a finite number are different from zero. Since each of these sums is formed from a finite number of nonzero terms and the coefficients $\alpha, \beta, \gamma, \cdots$ are rational and therefore form a countable set, it seems intuitively plausible that not only should the basis set be of the same power as the continuum but in some way be of the same "thickness" as the continuum. However, this intuitive feeling is seemingly contradicted by the only known results along this line, namely: the inner measure of a Hamel basis is zero and its outer measure may also be zero.[2] Nevertheless, this intuition is justified to some extent by Theorems 2, 4, and 5. A natural question arises: In order for a set of real numbers to contain a Hamel basis, what is both necessary and sufficient? For a certain family of sets (including the Borel and analytical sets) this question is answered in two ways. Certain other properties of a Hamel basis are investigated, the most interesting being an example of a Hamel basis which contains a nonvacuous perfect set. Finally, some rather curious discontinuous solutions of the equation $f(x)+f(y)=f(x+y)$ are given.

Measure. No Hamel basis of positive exterior measure is measurable.[3] The next few theorems show this to be true also of certain transforms of every Hamel basis.

DEFINITION. *If M is a set of real numbers, by $T(M)$ is meant the set of all numbers x' such that $x'=x+(y'-y)$, where x, y, and y' belong to M.*

With M considered as a linear set, $T(M)$ is the sum of all translations of M which intersect M. For convenience, $T[T(M)]$ is abbreviated $T^2(M)$, $T[T^2(M)]$ is abbreviated $T^3(M)$, and so on and $T^0(M)=M$.

Presented to the Society, September 2, 1941; received by the editors September 8, 1941.

[1] G. Hamel, *Eine Basis aller Zahlen und die unstetigen Lösungen der Funktionalgleichung: $f(x+y)=f(x)+f(y)$*, Mathematische Annalen, vol. 60 (1905), pp. 459–462.

[2] W. Sierpinski, *Sur la question de la mesurabilité de la base de M. Hamel*, Fundamenta Mathematicae, vol. 1 (1920), pp. 105–111.

[3] Ibid.

THEOREM 1. *If H is a Hamel basis, then for each positive integer n, $m_i T^n(H) = 0$.*[4]

PROOF. Suppose, on the contrary, that for some positive integer n, $m_i T^{n-1}(H) > 0$. Let a and b denote two numbers of H. Since the set of distances of the set $T^{n-1}(H)$ contains an interval with its left end at zero,[5] $T^n(H)$ contains an interval V whose midpoint is b. Since a/b is irrational and a is not zero, there exists a rational number r which is not an integer such that ra belongs to V and hence to $T^n(H)$. But every number of $T^n(H)$ can be expressed in the form $n_1x_1+n_2x_2+n_3x_3+\cdots$ where $x_1, x_2, x_3, \cdots$ belong to H and $n_1, n_2, n_3, \cdots$ are *integers* of which only a finite number are different from zero. This is contrary to the properties of H.

THEOREM 2. *If H is a Hamel basis, then for some positive integer n, $m_e T^n(H) > 0$.*

PROOF. Suppose, on the contrary, that for each positive integer n, $mT^n(H) = 0$. Hence $m\sum_0^\infty T^n(H) = 0$. Let M_0 denote $\sum T^n(H)$, and let a denote a fixed number of M_0. Evidently every number of the form $a+n_1(b-a)+n_2(c-a)+n_3(d-a)+\cdots$ (where $b, c, d, \cdots$ belong to H and $n_1, n_2, n_3, \cdots$ are integers of which only a finite number are different from zero) belongs to M_0. Hence the set of all numbers of this form are of measure zero. So the set of all numbers of the form $a+n_1(b-a)+n_2(c-a)+n_3(d-a)+\cdots+n_0a$ (where n_0 is an integer and all other symbols have the same meaning as before) is of measure zero. Now any real number x can be expressed in the form $\alpha a+\beta b+\gamma c+\cdots$ (where $\alpha, \beta, \gamma, \cdots$ are rational numbers of which only a finite number are different from zero) and hence there exists an integer q (which depends on x) such that $q\alpha, q\beta, q\gamma, \cdots$ are integers of which only a finite number are different from zero. Consequently, qx is of the form $a+n_1(b-a)+n_2(c-a)+n_3(d-a)+\cdots+n_0a$. It follows that the set of all real numbers x is of measure zero, which is false.

DEFINITION. *If M is a set of real numbers, then $D(M)$ denotes the set of all numbers $x-y$ where x and y belong to M and $x \geqq y$. The set $D(M)$ is called the set of distances of the set M.*[6]

---

[4] Throughout this paper, if Q is a set, m_iQ and m_eQ denote the interior measure and exterior measure, respectively, of Q and mQ denotes the measure of Q if measurable (in the sense of Lebesgue).

[5] H. Steinhaus, *Sur les distances des points des ensembles de mesure positive*, Fundamenta Mathematicae, vol. 1 (1920), pp. 93–104.

[6] Steinhaus, loc. cit.

THEOREM 3. *If H is a Hamel basis, then for each positive integer n, $m_i D^n(H)=0$.*

Theorem 3 may be established by substituting D for T in the proof of Theorem 1.

THEOREM 4. *If H is a Hamel basis, then for some positive integer n, $m_e D^n(H)>0$.*

PROOF. Suppose the contrary. Let $N=\sum_1^\infty D^n(H)$. Then $mN=0$. Let Q denote the set of all points of H which are limit points of H from both sides, and let M denote a countable subset of H such that (1) M contains $H-Q$ and (2) every point of $H-M$ is a limit point of M. It follows that each point of $H-M$ is a limit point of M from both sides. Let x denote a real number. Then x is of the form $\alpha a+\beta b+\gamma c+\cdots$ (where $a, b, c, \cdots$ belong to H and $\alpha, \beta, \gamma, \cdots$ are rational numbers of which only a finite number are different from zero). Hence there exists an integer q such that qx is of the form $n_1 a+n_2 b+n_3 c+\cdots$ (where $n_1, n_2, n_3, \cdots$ are integers of which only a finite number are different from zero). So qx is of the form $\sum_1^j e_i x_i$ (where for each i, $i=1, 2, \cdots, j$, x_i belongs to H and e_i is ± 1). For each integer i, $i=1, 2, \cdots, j$ (j is finite and depends on x), there exists a number y_i of M such that $\sum_1^j e_i(x_i-y_i)$ belongs to N.[7] Hence $qx=\bar{x}+\sum_1^j e_i y_i$ where $\bar{x}$ belongs to N. Since there are only countably many numbers of the form $\sum_1^j e_i y_i$, it follows that the set of all real numbers x is of measure zero, which is a contradiction.

LEMMA 1. *If M is a set of numbers and every number of some number interval V can be expressed in the form $\alpha a+\beta b+\gamma c+\cdots$ (where $a, b, c, \cdots$ belong to M and $\alpha, \beta, \gamma, \cdots$ are rational numbers of which only a finite number are different from zero), then M contains a Hamel basis.*

Lemma 1 may be established by well-ordering M and applying Hamel's argument to this well-ordering.

THEOREM 5. *If M is a set of real numbers and for some positive integer n, either $m_i T^n(M)>0$ or $m_i D^n(M)>0$, then M contains a Hamel basis.*

Theorem 5 follows from Lemma 1 and one of Steinhaus' theorems on the set of distances of a set.[8] The condition in Theorem 5 under

[7] This can be done by first choosing y_1 so that $e_1(x_1-y_1)\geqq 0$. This makes $e_1(x_1-y_1)$ belong to $D(H)$. If it is zero, choose y_2 so that $e_2(x_2-y_2)\geqq 0$; but if it is positive choose y_2 so that $e_2(x_2-y_2)\leqq 0$ but $e_1(x_1-y_1)+e_2(x_2-y_2)\geqq 0$. This makes $e_1(x_1-y_1)+e_2(x_2-y_2)$ belong to $D^2(H)$. Continue this process.

[8] Loc. cit., Theorem 8, p. 99.

which the set M contains a Hamel basis is not necessary. This can be seen from Theorems 1 and 3.

EXAMPLE 0. *The Cantor discontinuum*[9] *contains a Hamel basis, because its set of distances contains the interval from zero to one.*

DEFINITIONS. *Let F_T denote the family of all sets M of real numbers such that for infinitely many different positive integral values of n, $T^n(M)$ is measurable; and let F_D denote the family of all sets M of real numbers such that for infinitely many different positive integral values of n, $D^n(M)$ is measurable.*

THEOREM 6. *If M is a set of the family F_T, then in order that M contain a Hamel basis it is necessary and sufficient that for some positive integer n, $mT^n(M)>0$.*

THEOREM 7. *If M is a set of the family F_D, then in order that M contain a Hamel basis it is necessary and sufficient that for some positive integer n, $mD^n(M)>0$.*

LEMMA 2. *If M is an analytical set of real numbers, then both $T(M)$ and $D(M)$ are analytical sets.*

PROOF. Being an analytical set of real numbers, M is the set of values of a function $f_1(x)$ of a real variable, defined and continuous in the set of all irrational numbers.[10] Furthermore, $D(M)$ is analytical[11] and the set N consisting of all real numbers x such that either x or $-x$ belongs to $D(M)$ is an analytical set. Hence N is the set of values of a function $f_2(x)$ of a real variable, defined and continuous in the set of all irrational numbers. Let $f(x, y)\equiv f_1(x)+f_2(y)$ where x and y are irrational numbers. Then $T(M)$ is the set of values of $f(x, y)$ and $f(x, y)$ is defined and continuous in the set of all points of the number plane whose coordinates are both irrational numbers. It follows that $T(M)$ is analytical.[12]

Perfect sets, analytical sets. Since every analytical set is measurable,[13] the following three theorems may be easily established using Lemma 2 and Theorems 6 and 7.

[9] The subset of the interval from 0 to 1 (of real numbers) remaining after deleting in succession every middle-1/3 segment (open interval).

[10] W. Sierpinski, *Introduction to General Topology*, The University of Toronto Press, Toronto, 1930, translated by C. C. Krieger, Theorem 73, p. 145.

[11] W. Sierpinski, *Sur l'ensemble de distances entre les points d'un ensemble*, Fundamenta Mathematicae, vol. 7 (1925), pp. 144–148, p. 146 in particular.

[12] W. Sierpinski, *General Topology*, loc. cit., Theorem 89, p. 185.

[13] N. Lusin, *Leçons sur les ensembles analytiques*, Gauthier-Villars, Paris, 1930, p. 152.

THEOREM 8. *In order that an analytical set A of real numbers shall not contain a Hamel basis it is necessary and sufficient that for each positive integer n, both* $mT^n(A)$ *and* $mD^n(A)$ *be zero.*

THEOREM 9. *No Hamel basis is an analytical set.*

THEOREM 10. *If an analytical set M is a subset of a Hamel basis, then for each positive integer n, both* $mT^n(M)$ *and* $mD^n(M)$ *are zero.*

THEOREM 11. *Suppose that* $f(x)$ *is a discontinuous real function which is defined for all real values of x and which satisfies the equation* $f(x)+f(y)=f(x+y)$. *If* $f(x)$ *is bounded over the analytical set K of real numbers, then for each positive integer n,* $mT^n(K)=0$.

PROOF. Since $f(x)$ is bounded over K, there exists a positive number B such that $|f(x)|<B$ if x belongs to K. It follows from the elementary properties of $f(x)$ (which are imposed upon it by the functional equation) that for any positive integer n, $|f(x)|<3^nB$ if x belongs to $T^n(K)$. Suppose that for some integer $\bar{n}$, $mT^{\bar{n}}(K)\neq 0$. Since $T^{\bar{n}}(K)$ is analytical, it is measurable, and hence, is of *positive* measure. Then $T^{\bar{n}+1}(K)$ contains an interval. Since $f(x)$ is bounded over this interval, by one of Darboux's theorems it must be continuous.[14] This is a contradiction.

COROLLARY 1. *If the discontinuous solution* $f(x)$ *of the functional equation* $f(x)+f(y)=f(x+y)$ *is continuous in an analytical set K of real numbers, then for each positive integer n,* $mT^n(K)=0$.

COROLLARY 2. *Suppose that A is an analytical subset of the plane image of a discontinuous solution of the equation* $f(x)+f(y)=f(x+y)$ *and that K is the projection of A onto the x-axis. Then for each positive integer n,* $mT^n(K)=0$.

THEOREM 12. *No discontinuous solution of the equation* $f(x)+f(y)=f(x+y)$ *is continuous in an analytical set which contains a Hamel basis.*

Theorem 12 follows immediately from Theorem 8 and Corollary 1.

Remarks and examples. Burstin showed the existence of a Hamel basis H which intersects every perfect set of real numbers.[15] It fol-

---

[14] Darboux, *Sur la composition des forces in statique*, Bulletin des Sciences Mathématiques, vol. 9 (1875), p. 281.

[15] C. Burstin, *Die Spaltung des Kontinuum in c in L Sinne nichtmessbare Mengen*, Sitzungsberichte der Akademie der Wissenschaften. Vienna, Mathematisch-naturwissenschaftliche Klasse, Abt. IIa, vol. 125 (1916).

lows that H does not contain a perfect set. But every uncountable analytical set contains a perfect set.[16] Consequently, this particular Hamel basis H does not contain an uncountable analytical set. This example and Theorems 9 and 10 might lead one to conjecture that no Hamel basis whatsoever contains an uncountable analytical set. That this conjecture would be false is shown by the following example.

EXAMPLE 1. *There exists a Hamel basis which contains a perfect set.*[17]

CONSTRUCTION. Let $r_1, r_2, r_3, \cdots$ denote a simple well-ordering of the rational numbers such that $r_1=0$. Let I_{11} denote a closed interval of real numbers not containing zero. The interval I_{11} contains two intervals I_{21} and I_{22} such that (1) I_{21} precedes I_{22} and (2) no number of the form $n_1x_1+n_2x_2$ except the forms x_1 or x_2 belongs to $I_{21}+I_{22}$, where $x_1, x_2 \in I_{21}+I_{22}$ and where $n_i=r_j$, $i, j=1$ or 2. Likewise I_{21} contains two intervals I_{31} and I_{32}, and I_{22} contains two intervals I_{33} and I_{34} such that (1) I_{31} and I_{33} precede I_{32} and I_{34}, respectively, and (2) no number of the form $n_1x_1+n_2x_2+n_3x_3$ except the forms x_1, x_2, or x_3 belongs to $\sum I_{3n}$ where $x_1, x_2, x_3 \in \sum I_{3n}$ and where $n_i=r_j$, $i, j=1, 2$, or 3. This process may be continued. For each positive integer k, let G_k denote the collection of mutually exclusive intervals $I_{k1}, I_{k2}, \cdots, I_{kq}$, where $q=2^{k-1}$. For each k, each element of G_k contains two elements of G_{k+1} and if $x_1, x_2, \cdots, x_k$ denote numbers of G_k^*, then no number of the form $\sum_1^k n_ix_i$ except the form x_i belongs to G_k^*, where $n_i=r_j$, $i, j=1, 2, \cdots, k$.[18] Now let M denote $\prod_1^\infty G_i^*$. Evidently M is a perfect set such that if $\bar{x}$ is a number of M, then $\bar{x} \neq \alpha A+\beta B+\gamma C+\cdots$ where $A, B, C, \cdots$ are numbers of $M-\bar{x}$ and $\alpha, \beta, \gamma, \cdots$ are rational numbers of which only a finite number are different from zero. It follows from this that if $\bar{x}$ is a real number which can be expressed in the form $\alpha A+\beta B+\gamma C+\cdots$ where $A, B, C, \cdots$ belong to M and $\alpha, \beta, \gamma, \cdots$ are rational numbers of which only a finite number are different from zero, then it can be thus expressed in only one way, that is, the form is unique.

Let Γ denote a well-ordering of the real numbers not belonging to M and let a denote the first number of Γ which is not of the form $\alpha A+\beta B+\gamma C+\cdots$ where $A, B, C, \cdots$ belong to M and $\alpha, \beta, \gamma, \cdots$ are rational numbers of which only a finite number are different from

[16] Lusin, loc. cit., p. 151.

[17] R. L. Swain, in a conversation with me, demonstrated the existence of a perfect set whose set of distances contains no rational number. His method of construction forms the kernel of the one that I use here.

[18] G_k^* denotes the sum of the elements of G_k.

zero. Let b denote the first number of Γ which is not of the form $\alpha A+\beta B+\gamma C+\cdots$ where $A, B, C, \cdots$ belong to $M+a$. This process may be continued. It follows from Hamel's argument that $M+a+b+c+\cdots$ is a Hamel basis.[19]

Since, from Theorem 11, no discontinuous (real) solution of the functional equation $f(x)+f(y)=f(x+y)$ can be continuous at any point or continuous in any set of positive measure, could such a discontinuous solution be continuous in some *perfect* set? And could its image in the number plane (the graph of $y=f(x)$) at the same time be *connected*? Example 2 shows that the answer is *yes*.

EXAMPLE 2. *There exist a discontinuous (real) solution of the functional equation $f(x)+f(y)=f(x+y)$ and a perfect set M of real numbers such that (1) $f(x)=0$ if x belongs to the perfect set M and (2) the plane image of $f(x)$ is connected.*

CONSTRUCTION. Let M denote a perfect subset of a Hamel basis H such that $H-M$ contains a perfect set. For each number x of M, let $f(x)$ be defined to be zero. Define the function $f(x)$ for each of the numbers of $H-M$ in such a way so that if Q is a continuum in the number plane not lying wholly in a vertical line, then for some number x of $H-M$, the point $(rx, rf(x))$ belongs to Q.[20] Now if x is any number not belonging to H, $x=\alpha a+\beta b+\gamma c+\cdots$ where $a, b, c, \cdots$ belong to H and $\alpha, \beta, \gamma, \cdots$ are rational numbers of which only a finite number are different from zero. Let $f(x)=\alpha f(a)+\beta f(b)+\gamma f(c)+\cdots$. It follows from Hamel's argument that $f(x)$ satisfies the functional equation.[21] Furthermore, $f(x)$ has the following properties: (0) $f(x)$ is totally discontinuous but (1) $f(x)$ is zero for all numbers in the perfect set M and (2) the plane image of $f(x)$ is connected.[22]

In order for the plane image I of *any* discontinuous solution of $f(x)+f(y)=f(x+y)$ to be connected, I must intersect every[23] continuum in the plane which does not lie in some vertical line. However, I need not intersect every perfect subset of the plane not lying in the sum of a countable number of vertical lines, for the image of $f(x)$ in Example 2 does not contain any point of the line $y=1$ whose abscissa belongs to M. So by virtue of the fact that I may be connected and

---

[19] G. Hamel, loc. cit. $M+a+b+c+\cdots$ denotes the sum of the *sets*, $M, a, b, c, \cdots$.

[20] F. B. Jones, *Connected and disconnected plane sets and the functional equation* $f(x)+f(y)=f(x+y)$, this Bulletin, vol. 48 (1942), pp. 115–120, Theorems 2 and 4; r is rational.

[21] G. Hamel, loc. cit.

[22] F. B. Jones, loc. cit.

[23] Ibid., Theorem 2.

still *contain* a perfect set not lying in the sum of countably many vertical lines, it follows that I need not *intersect* every such perfect set. Since, by Theorem 11, Corollary 2, I can *not* contain a perfect set whose projection on the x-axis is of positive measure, one might suppose that I must intersect every such perfect set in order to be connected. The following example shows this supposition to be false.

EXAMPLE 3. *There exists a discontinuous solution of the equation* $f(x)+f(y)=f(x+y)$ *such that* (1) *the image* I *of* $f(x)$ *in the number plane* E *is connected but* (2) *the intersection of* I *with the* x*-axis is exactly the set of rational numbers.*

Two lemmas are necessary.

LEMMA 3. *Suppose that* M *is a bounded, closed subset of the number plane. If uncountably many horizontal lines intersect* M *in an uncountable set, then each of* c *horizontal lines intersects* M *in an uncountable set.*[24]

PROOF. Let E denote the number plane. Let W denote the set of all points w of the y-axis for which there exist sets M_w such that (1) M_w is a subset both of a horizontal line in E through w and of M and (2) every point of M_w is a point of condensation of M_w from both sides. There exists a pair of vertical lines L_{11} and L_{12} (L_{11} being to the left of L_{12}) and an uncountable subset W_1 of W such that for each element w of W_1, M_w contains points between L_{11} and L_{12}, to the left of L_{11} and to the right of L_{12}. Let P_{11} denote a point of M lying between L_{11} and L_{12} such that for uncountably many different elements w of W_1, M_w is a subset of a horizontal line lying above P_{11} in E and for uncountably many elements w of W_1, M_w is a subset of a horizontal line lying below P_{11} in E. Let W_1^+ and W_1^- denote the set of all of those elements w of W_1 for which M_w is on a line above P_{11} and below P_{11}, respectively. Select one of the sets W_1^+ and W_1^- and denote the selection by $W_1^\pm$. Then there exist vertical lines L_{21}, L_{22}, L_{23}, and L_{24} having that order from left to right (with P_{11} between L_{22} and L_{23}) and an uncountable subset W_2 of $W_1^\pm$ such that for each w of W_2, M_w has points to the left of L_{21}, between L_{21} and L_{22}, between L_{22} and the vertical line through P_{11}, between this line and L_{23}, between L_{23} and L_{24}, and to the right of L_{24}. Let P_{21} and P_{23} denote two points of M which lie on the same horizontal line such that uncountably

[24] c is the cardinal number of the continuum. It would follow from this lemma that any closed subset of the plane which cannot be covered by a countable collection of horizontal and vertical lines can be covered only by a collection of horizontal and vertical lines which contains at least c lines.

many elements of W_2 lie above and uncountably many elements of W_2 lie below this line, denoting them by W_2^+ and W_2^-. Select *one* of the sets W_2^+ and W_2^- and denote the selection by $W_2^\pm$. This process may be continued and an infinite sequence of points P_{11}, P_{21}, P_{22}, P_{31}, P_{33}, P_{35}, P_{37}, $\cdots$ obtained whose limiting set Q is uncountable and lies both in M and in a horizontal line. Since for each n, $n=2, 3, 4, \cdots$ there are *two* selections possible in the selection of $W_n^\pm$, there are $2^{\aleph_0}$ such limiting sets of which no three are identical. Hence there are c different such sets Q.

LEMMA 4. *No compact continuum M lying in the number plane which is not wholly in a vertical line and whose common part with every horizontal line is totally disconnected is a subset of the sum of less than c vertical and horizontal lines.*

Lemma 4 may be established by an indirect argument with the help of Lemma 3 and the fact that an uncountable closed plane set contains c points.

CONSTRUCTION OF EXAMPLE 3. Let Γ denote a well-ordering of type Ω_0 (Ω_0 is the smallest ordinal having c ordinals less than it) of the set of all nondegenerate compact subcontinua of E not lying in a vertical line and let $x_1, x_2, x_3, \cdots, x_\omega, x_{\omega+1}, \cdots, x_z, \cdots, z<\Omega_0$, denote a well-ordering of a Hamel basis H such that $x_1=1$ and H contains a number of every perfect set of real numbers. Let $y_1=f(x_1)=f(1)=0$. If r is a rational number, let $f(r)=rf(1)=0$. Suppose that, for each ordinal $z<z_0<\Omega_0$, $f(x_z)$ is defined to be a number y_z. Then if $x=\sum r_z x_z$, $z<z_0$, $f(x)=\sum r_z y_z$, $z<z_0$, where r_z is a rational number and *not* zero for only a finite number of different values of z. Let I_{z_0} denote the image of $f(z)$ as defined so far. Let M_{z_0} denote the first element of Γ which contains no point of I_{z_0}. Let z_1 denote the smallest ordinal such that (1) $f(x_{z_1})$ is not defined so far and (2) there exists a number y_{z_1} such that (x_{z_1}, y_{z_1}) belongs to M_{z_0} and y_{z_1} is not the ordinate of any point of I_{z_0}. Since $z<\Omega_0$, the existence of z_1 may be established with the help of Lemma 4 and the theorem that every uncountable inner-limiting set of real numbers contains c mutually exclusive perfect sets. Then let $f(x_{z_1})=y_{z_1}$. If $\bar{z}$ is an ordinal less than z_1 such that for each ordinal $z<\bar{z}$, $f(x_z)$ is defined to be y_z, then let $f(x_{\bar{z}})$ be a real number $y_{\bar{z}}$ such that $y_{\bar{z}}$ is not $r_{z_1}y_{z_1}+\sum r_z y_z$, $z<\bar{z}$, where r_z is a rational number which is different from zero for only a finite number of different values of z and r_{z_1} is a rational number.

This completes the induction in the definition of $f(x)$ if x belongs to H. If x is any real number, then $x=\sum r_z x_z$, where r_z is a rational number which is different from zero for only a finite number of differ-

ent values of z. This expression for x being unique, $f(x)$ is defined to be $\sum r_z y_z$. By Hamel's argument[25] $f(x)$ satisfies the equation $f(x)+f(y)=f(x+y)$. Obviously the image I of $f(x)$ intersects every compact subcontinuum of E not in a vertical line and hence intersects every such subcontinuum of E whether compact or not. Hence I is connected.[26] Suppose that for two different numbers a_1 and a_2, $f(a_1)=f(a_2)$. But $a_1=\sum r_{1z}x_z$ and $a_2=\sum r_{2z}x_z$, where r_{1z} and r_{2z} are rational numbers which are different from zero for only a finite number of different values of z. Hence $\sum r_{1z}y_z=\sum r_{2z}y_z$. Let $\bar{z}$ be the largest value of z such that $r_{1z}-r_{2z}\neq 0$. Then $y_z=\sum y_z(r_{2z}-r_{1z})/(r_{1\bar{z}}-r_{2\bar{z}})$, $z<\bar{z}$. This however is impossible if $\bar{z}>1$. Hence $r_{1z}-r_{2z}=0$ if $z>1$ and $a_1=a_2=r_{11}-r_{21}$. It follows from this that if L is a horizontal line intersecting I at the point (x, y) then $I\cdot L$ is the set of all points $(x+r, y)$ where r is rational.

THE UNIVERSITY OF TEXAS

[25] Loc. cit.

[26] See Footnote 23.

ON THE COMPOSITION OF FIELDS

CLAUDE CHEVALLEY

Let K/k, K'/k be two extensions of a basic field k. By a *composite extension* of these two extensions, we understand the complex notion formed of an extension Ω/k of k, of an isomorphism τ of K/k into Ω/k and of an isomorphism τ' of K'/k into Ω/k, provided the following conditions are verified:

(1) Ω is generated by the two fields K^{τ}, $K'^{\tau'}$.

(2) If A, A' are subsets of K, K' respectively which are algebraically independent over k, the set $A^{\tau} \cup (A')^{\tau'}$ is algebraically independent over k. In other words, the algebraic relations which hold in Ω between elements of K^{τ}, $K'^{\tau'}$ are consequences of the algebraic relations which hold between elements of K^{τ} alone or of $K'^{\tau'}$ alone.[1]

THEOREM 1. *Any two given extensions K/k, K'/k have at least one composite extension.*

Let B' be a transcendence basis for K'/k. We can find a purely transcendental extension Ω/K which has a transcendence basis $B'^{\tau'}$ with the same cardinal number as B' (τ' stands for a one-to-one mapping of B' onto $B'^{\tau'}$). The algebraic closure $\bar{\Omega}$ of Ω contains the algebraic closure $\bar{\mathrm{P}}$ of the field $\mathrm{P} = k(B'^{\tau'})$. The mapping τ' may be extended to an isomorphism of K'/k with an extension $K'^{\tau'}/k$ contained in $\bar{\mathrm{P}}/k$, and a fortiori in $\bar{\Omega}$. We set $\Omega = KK'^{\tau'}$, and denote by τ the identity mapping of K/k into Ω/k. We claim that the system $(\Omega/k, \tau, \tau')$ is a composite extension of K/k, K'/k.

It is sufficient to check the condition (2), and we may assume without loss of generality that A, A' are finite. There exists a finite subset B_1' of B' such that $k(A', B_1')$ is algebraic over $k(B_1')$. Let d, d', e be the number of elements in A, A_1', B_1'. The elements of B_1', being algebraically independent over K, are *a fortiori* algebraically independent over $k(A)$. Therefore, the degree of transcendency of $k(A, A'^{\tau'}, B_1'^{\tau'})$ over k is $d+e$. The degree of transcendency of $k(A_1'^{\tau'}, B_1'^{\tau'})$ over $k(A_1'^{\tau'})$ is $e-d'$. The degree of transcendency f of $k(A, A'^{\tau'}, B_1'^{\tau'})$ over $k(A)$ is therefore less than or equal to $e-d$. It follows that the degree of transcendency of $k(A, A'^{\tau'})$ over k, which

Received by the editors October 1, 1941.

[1] The problem of composite extensions has been considered by Zariski (*Algebraic varieties over ground fields of characteristic zero*, American Journal of Mathematics, vol. 62 (1940), pp. 187–221) in the case when one of the extensions K/k, K'/k is algebraic and normal.

is $d+e-f$, is at least equal to $d+d'$, which proves that $A \cup A'^{\tau'}$ is algebraically independent over k.

Let $(\mathfrak{K}/k, \tau, \tau')$ and $(\mathfrak{K}_1/k, \tau_1, \tau_1')$ be two composite extensions of K/k, K'/k. We shall say that these extensions are isomorphic if there exists an isomorphism σ of $\mathfrak{K}/k$ with $\mathfrak{K}'/k$ such that $\tau_1 = \sigma\tau$, $\tau_1' = \sigma\tau'$.

The consideration of the case where K/k, K'/k are algebraic over k (but not normal) shows immediately that there are in general several non-isomorphic types of composite extensions. The extreme opposite case occurs when k is algebraically closed in K and K' (k is said to be algebraically closed in K if every element of K which is algebraic over k lies already in k). In that case, the composite extension $\mathfrak{K}/k$ turns out to be unique; but, unfortunately, k may fail to be algebraically closed in $\mathfrak{K}$. For instance, let us take $K = K' = k(x, (a+bx^p)^{1/p})$, where $p \neq 0$ is the characteristic of k, and where a, b are elements of k such that $k((a)^{1/p}, (b)^{1/p})$ is of degree p^2 over k. It is easy to verify that k is algebraically closed in K; on the other hand, the composite extension is $k(x, y, (a+bx^p)^{1/p}, (a+by^p)^{1/p})/k = k(x, y, (a)^{1/p}, (b)^{1/p})/k$.

We shall get around this difficulty by introducing the following notion:

DEFINITION 1. *A field k is said to be quasi-algebraically closed (q.a.c.) in K if every element a of K which is algebraic over k is purely inseparable over k (that is, is the unique root of some equation with coefficients in k).*

We shall prove the following theorem:

THEOREM 2. *Let $(\mathfrak{K}/k, \tau, \tau')$ and $(\mathfrak{K}_1/k, \tau_1, \tau_1')$ be two composite extensions of the extensions K/k, K'/k. Let L, L' be fields such that: (1) $k \subset L \subset K$, $k \subset L' \subset K'$; (2) L, L' are algebraic over k; (3) L is q.a.c. in K and L' is q.a.c. in K'. If an isomorphism σ_0 of $L^\tau L'^{\tau'}/k$ with $L^{\tau_1} L'^{\tau_1'}/k$ is such that $\sigma_0\tau$ coincides on L with τ_1 and $\sigma_0\tau'$ coincides on L' with τ_1', then σ_0 may be extended to an isomorphism of $(\mathfrak{K}/k, \tau, \tau')$ with $(\mathfrak{K}_1/k, \tau_1, \tau_1')$.*

In other words, the type of the composite extension $(\mathfrak{K}/k, \tau, \tau')$ is determined by the type of the composite extension $(L^\tau L'^{\tau'}/k, \tau, \tau')$ of L/k, L'/k.

We shall first prove three lemmas. The fields which are considered in the first two of these lemmas are assumed to be all subfields of some all-inclusive field.

LEMMA 1. *Let k be a q.a.c. sub-field of a field K. Let Z be a field such that $k \subset Z \subset K$, and y be an element of K which is a root of an irreducible equation $F = 0$ with coefficients in Z. Let Ω/k be an algebraic extension*

of k, α be an element of Ω and $\Phi=0$, the irreducible equation in k which is satisfied by α. Then the polynomial F is a power of an irreducible polynomial in the field ΩZ, and Φ is a power of an irreducible polynomial in K. Moreover, Ω is q.a.c. in the field $K\Omega$.

We may assume without loss of generality that $\Omega=k(\alpha)$. Let L be the algebraic closure of k in K (that is, the field consisting of the elements of K which are algebraic over k). Let $\Phi_1=0$ be the irreducible equation satisfied by α in L. Therefore Φ_1 divides Φ. On the other hand, if p is the characteristic of k, the polynomial $\Phi_1^{p^u}$ has its coefficients in k if u is large enough, and therefore Φ divides $\Phi_1^{p^u}$. It follows that Φ is a power of Φ_1.

If $\Phi_1'=0$ is the irreducible equation satisfied by α in K then Φ_1' divides Φ_1. Therefore, every root of the equation $\Phi_1'=0$ is also a root of $\Phi_1=0$, which shows that the coefficients of Φ_1' are algebraic over k. It follows that $\Phi_1'=\Phi_1$ which proves that Φ is a power of an irreducible polynomial in K.

Let $F_1=0$ be the irreducible equation satisfied by y in LZ, and let m be the degree of F_1. If n is the degree of ϕ_1, we have

$$[LZ(y,\alpha):LZ]=[LZ(y,\alpha):LZ(y)][LZ(y):LZ]=mn$$

because Φ_1 is irreducible in K, and *a fortiori*, in $LZ(y)$. It follows that

$$[LZ(y,\alpha):LZ(\alpha)][LZ(\alpha):LZ]=mn.$$

But $[LZ(\alpha):LZ]=n$, since Φ_1 is irreducible in LZ; therefore we have $[LZ(y,\alpha):LZ(\alpha)]=n$ which shows that F_1 is irreducible in $LZ(\alpha)$. On the other hand, F_1 divides F; since LZ is purely inseparable over Z, the same argument which was used above for Φ_1 shows that F is a power of F_1. Since $Z\subset\Omega Z=Z(\alpha)\subset LZ(\alpha)$, F is also a power of an irreducible polynomial in ΩZ.

There remains to prove that $k(\alpha)$ is q.a.c. in $K(\alpha)$. Let β be an element of $K(\alpha)$ which is algebraic over $k(\alpha)$, and therefore also on k. There exists a power $\alpha^{p^s}=\alpha_1$ of α which is separable over k; we set $\beta_1=\beta^{p^s}$, whence $\beta_1\in K(\alpha_1)$ and

$$\beta_1=\xi_0+\xi_1\alpha_1+\cdots+\xi_{h-1}\alpha_1^{h-1},\qquad \xi_i\in K,$$

where $h=[K(\alpha_1):K]$. If we write the corresponding formulas for the conjugates of β_1 with respect to K, and observe that α_1 is different from its conjugates, we see that the ξ_i's may be expressed rationally by means of the conjugates of α_1, β_1. It follows that $\xi_0, \xi_1, \cdots, \xi_{h-1}$ are algebraic over k, and therefore belong to L. Since L is purely in-

separable over k, we may conclude that some power $\beta_1^{p^t}$ of β_1 lies in $k(\alpha_1)$, where p is the characteristic of k ($\beta_1 \in k(\alpha_1)$) (if $p=0$). We have $\beta^{p^{s+t}} \in \Omega$ which completes the proof of the lemma.

Before stating Lemma 2, we have to introduce another notion. Two extensions K/k, Ω/k of the field k which are contained in some larger field are said to be *algebraically dissociated* if the following condition is realized: If A, B are subsets of K, Ω, respectively, which are algebraically independent over k, the set $A \cup B$ is also algebraically independent.

LEMMA 2. *The Lemma* 1 (*abstraction made of what concerns* α *and* Φ) *remains valid when* Ω/k *is any extension of* k, *provided the extensions* Ω/k, K/k *are algebraically dissociated.*

Let C be a transcendence basis of Ω/k and Ω_0 the field $k(C)$. Under our assumption the extension $K\Omega_0/K$ is purely transcendental. We claim that Ω_0 is q.a.c. in $K\Omega_0$. It will of course be sufficient to prove it in the case where C consists[2] in a single element t. Let $P(t)/Q(t)=\omega$ be an element of $K\Omega_0=K(t)$ (where $P(t)$, $Q(t)$ are polynomials with coefficients in K). We shall prove that if ω is algebraic over Ω_0, it can be expressed as a rational function in t with coefficients in L (the algebraic closure of k in K). From this result it will follow that $L\Omega_0$ is algebraically closed in $K\Omega_0$, and therefore that Ω_0 is q.a.c. in $K\Omega_0$.

The proof will proceed by induction on the number $l=d^\circ P+d^\circ Q$ where $d^\circ P$, $d^\circ Q$ denote the degrees of P, Q with respect to t. It is obvious for $l=0$; assume that the result holds for $l-1$. If either one of the elements $P(0)$, $Q(0)$ is null, we can reduce ourselves to the case $l-1$ by considering instead of ω one of the elements ω/t, $t\omega$ (these elements are also algebraic over Ω_0). So, let us assume that $P(0)Q(0)\neq 0$. We have by assumption a relation of the form

$$A_0(t)P^n(t) + A_1(t)P^{n-1}(t)Q(t) + \cdots + A_n(t)Q^n(t) = 0,$$

where $A_0(t), \cdots, A_n(t)$ are polynomials in t with coefficients in k, not all divisible by t. Putting $t=0$, we conclude that $P(0)/Q(0)$ is algebraic over k, and therefore belongs to L. The element $\omega' = P(t)/Q(t) - P(0)/Q(0)$ is again algebraic over Ω_0 and may be written in the form $tP'(t)/Q'(t)$ with $d^\circ P' + d^\circ Q' = l-1$. Therefore $\omega'/t \in L(t)$ and $\omega \in L(t)$, which proves our assertion.

The extension $Z\Omega_0/Z$ being purely transcendental (because $K\Omega_0/K$ is), the polynomial F, which is irreducible in Z, remains irreducible

[2] This property was proved in the paper, *Pencils on an algebraic variety and a new proof of a theorem of Bertini*, by Zariski, Transactions of this Society, vol. 50 (1941), pp. 48–70.

in $Z\Omega_0$. The extension Ω/Ω_0 being algebraic, it follows from Lemma 1 (applied with Ω_0 instead of k) that F becomes a power of an irreducible polynomial in $Z\Omega$ and that Ω is q.a.c. in $K\Omega$; Lemma 2 has been proved.

We pass now to the third lemma. The notations used in this lemma are the same as those introduced in the statement of Theorem 2.

LEMMA 3. *Let Z be a field such that $L \subset Z \subset K$, and let y be an element of K.* (1) *If y is transcendental over Z, y^r is transcendental over $Z^r K'^{r'}$.* (2) *If y is a root of the irreducible equation $F=0$ in Z, the polynomial F^r is a power of an irreducible polynomial in $Z^r K'^{r'}$.*

(1) Let B' be a transcendence basis of K'/k and C be a transcendence basis of Z/k; hence $C^r \cup B'^{r'}$ is a transcendence basis of $Z^r K'^{r'}/k$. If y is transcendental over Z, the set $C \cup \{y\}$ is algebraically independent; therefore $C^r \cup B'^{r'} \cup \{y^r\}$ is algebraically independent over k, which proves that y^r is transcendental over $Z^r K'^{r'}$.

(2) Since the extensions Z^r/k, $K'^{r'}/k$ are clearly algebraically dissociated over k, assertion (2) results from Lemma 2.

We pass now to the proof of Theorem 2. We consider the set Σ of the systems $(Z, Z', \sigma(Z, Z'))$ composed (a) of fields Z, Z' such that $L \subset Z \subset K$, $L' \subset Z' \subset K'$; (b) of an isomorphism $\sigma(Z, Z')$ of $Z^r Z'^{r'}$ with $Z^{r_1} Z'^{r_1'}$ such that $\sigma(Z, Z')\tau$ coincides with τ_1 on Z, that $\sigma(Z, Z')\tau'$ coincides with τ_1' on Z', and that $\sigma(Z, Z')$ coincides with σ_0 on $L^r L'^{r'}$. We order the set Σ by the convention that

$$(Z, Z', \sigma(Z, Z')) \leqq (U, U', \sigma(U, U'))$$

if $Z \subset U$, $Z' \subset U'$ and $\sigma(U, U')$ coincides with $\sigma(Z, Z')$ on $Z^r Z'^{r'}$. It is trivial to verify that in this ordered set every completely ordered subset has an upper bound. Hence, by Zorn's theorem, Σ has a maximal element, which we denote from now on by (Z, Z', σ). Theorem 2 will be proved if we can show that $Z=K$, $Z'=K'$.

Let y be an element of K, and assume for a moment that y is transcendental over Z. Then y^r is transcendental over Z^r and y^{r_1} is transcendental over Z^{r_1}. By Lemma 3, y is also transcendental over $Z^r Z'^{r'}$, and *a fortiori*, over $Z^r Z'^{r'}$. Similarly, y^{r_1} is transcendental over $Z^{r_1} Z'^{r_1'}$. We set $U=Z(y)$; then it is possible to extend σ to an isomorphism σ^* of $U^r Z'^{r'}$ with $U^{r_1} Z'^{r_1'}$ in such a way that $\sigma^*(y^r)=y^{r_1}$. It follows that $\sigma^*\tau$ coincides with τ_1 on U and that $\sigma^*\tau'$ coincides with τ_1' on Z'. But this is contrary to the maximality of (Z, Z', σ).

It follows that K is algebraic over Z, and similarly that K' is algebraic over Z'.

Let us again consider the element $y \in K$; it is a root of an irreducible

equation $F=0$ in Z. By Lemma 3, F^{τ} becomes in $Z^{\tau}Z'^{\tau'}$ a power of an irreducible polynomial F_1, and we have $F_1(y^{\tau})=0$. The polynomial F_1^{σ} is irreducible in $Z^{\tau_1}Z'^{\tau_1'}$, and $F^{\sigma\tau}$ is a power of F_1^{σ}. On the other hand, we have $F^{\sigma\tau}=F^{\tau_1}$ and $F^{\tau_1}(y^{\tau_1})=0$, whence $F_1^{\sigma}(y^{\tau_1})=0$. Therefore, we may extend σ to an isomorphism σ^* of $Z^{\tau}Z'^{\tau'}(y^{\tau})$ with $Z^{\tau_1}Z'^{\tau_1'}(y^{\tau_1})$ such that $\sigma^*(y^{\tau})=y^{\tau_1}$. The isomorphism $\sigma^*\tau$ of $Z(y)$ into $K^{\tau_1}K'^{\tau_1'}$ coincides with the automorphism induced by τ_1 and $\sigma^*\tau'$ coincides on Z' with τ_1'. By the maximality property of (Z, Z', σ), we have $Z(y)=Z$, whence $K=Z$, and we see in the same way that $K'=Z'$, which completes the proof of Theorem 2.

COROLLARY. *Let K/k, K'/k be two extensions of k, and assume that k is q.a.c. in at least one of them. Then there exists only one type of composite extension of our two extensions.*

In fact, if k is q.a.c. in K', we may apply Theorem 2 with $L'=k'$. If we set $\sigma_0=\tau_1\tau^{-1}$, σ_0 is an isomorphism of L^{τ} with L^{τ_1} and $\sigma_0\tau$ coincides with τ_1 on L; it follows that σ_0 may be extended to an isomorphism of $(\mathfrak{K}, \tau, \tau')$ with $(\mathfrak{K}_1, \tau_1, \tau_1')$.

THEOREM 3. *Let $(\mathfrak{K}/k, \tau, \tau')$ be a composite extension of K/k, K'/k and let L, L' be fields which satisfy the conditions* (1), (2), (3) *of Theorem 2. Then $L^{\tau}L'^{\tau'}$ is q.a.c. in $\mathfrak{K}$.*

By Lemma 1, $L^{\tau}L'^{\tau'}$ is q.a.c. in $L^{\tau}K'^{\tau'}$; by Lemma 2, we see that $L^{\tau}K'^{\tau'}$ is q.a.c. in $K^{\tau}K'^{\tau'}$, because the extensions K^{τ}/k, $K'^{\tau'}/k$ are algebraically dissociated. Let α be an element of $\mathfrak{K}$ which is algebraic over $L^{\tau}L'^{\tau'}$; then, if p is the characteristic of k, the second result shows that, for s large enough, $\alpha^{p^s}\in L^{\tau}K'^{\tau'}$. Since α^{p^s} is also algebraic over $L^{\tau}L'^{\tau'}$, the first result shows that $(\alpha^{p^s})^{p^{s'}}=\alpha^{p^{s+s'}}\in L^{\tau}L'^{\tau'}$, for s' large enough, which proves Theorem 3.

COROLLARY. *If k is q.a.c. in both K and K', it is also q.a.c. in $K^{\tau}K'^{\tau'}$.*

PRINCETON UNIVERSITY

NOTE ON CLOSURE FOR ORTHOGONAL POLYNOMIALS

J. SHOHAT

In this short note we give a simple theorem concerning closure for orthogonal polynomials (OP). The importance of closure in the theory of OP, particularly in the study of expansions of functions in series of OP, can hardly be overestimated.

The notations employed below are those of my monograph, *Théorie générale des polynômes orthogonaux de Tchebicheff* (Mémorial des Sciences Mathématiques, vol. 66, 1934), referred to as M.

We write generally

$$f(x) \sim \sum_{n=0}^{\infty} f_n \phi_n(x)$$

to signify that

$$f_n = \int_a^b f(x)\phi_n(x)d\psi, \qquad n = 0, 1, 2, \cdots,$$

$$\phi_n(x) \equiv \phi_n(x; a, b; d\psi),$$

$$\int_a^b \phi_m(x)\phi_n(x)d\psi = \delta_{mn}, \quad m, n = 0, 1, 2, \cdots.$$

The hereafter assumed existence of $\int_a^b f^2(x)d\psi$ implies, as is known, the convergence of the series $\sum_{n=0}^{\infty} f_n^2$. By closure we mean the following equality, Parseval's formula:

$$\int_a^b f^2(x)d\psi = \sum_{n=0}^{\infty} f_n^2.$$

THEOREM. *If closure holds for the "symmetric" sequence*

$$\{\phi_n(x; -h, h; d\psi)\}, \qquad \psi(\infty) - \psi(x) \equiv \psi(-x) \tag{1}$$

[*or*

$$\{\phi_n(x; -h, h; p(x))\}, \qquad p(x) \equiv p(-x)]$$

then each of the following two sequences of OP is closed

$$\{\phi_n(x; 0, h^2; d\psi_1)\}, \qquad \{\phi_n(x; 0, h^2; d\psi_2)\} \tag{2}$$

$$d\psi_1(x) = 2d\psi(x^{1/2}), \qquad d\psi_2(x) = x d\psi_1(x)$$

[*or*

Received by the editors October 2, 1941.

$$\{\phi_n(x; 0, h^2; p_1(x))\}, \qquad \{\phi_n(x; 0, h^2; p_2(x))\}$$
$$p_1(x) = x^{-1/2}p(x^{1/2}), \qquad p_2(x) = xp_1(x)],$$

and conversely.

It suffices to give the proof for $d\psi(x)$ proper, for the case where $d\psi(x) = p(x)dx$ is quite similar.

We have, for any $n = 0, 1, 2, \cdots$ [M, pp. 19–20],

$$\begin{aligned} \phi_{2n}(x; -h, h; d\psi) &\equiv \phi_n(x^2; 0, h^2; d\psi_1), \\ \phi_{2n+1}(x; -h, h; d\psi) &\equiv x\phi_n(x_n^2; 0, h^2; d\psi_2). \end{aligned} \tag{3}$$

This yields at once, for any $n = 0, 1, 2, \cdots$,

$$\begin{aligned} f_{2n} &= \int_{-h}^{h} f(x)\phi_{2n}(x; -h, h; d\psi)d\psi \\ &= \int_0^{h^2} F_1(x)\phi_n(x; 0, h^2; d\psi_1)d\psi_1 \equiv f_{n,1}, \\ f_{2n+1} &= \int_{-h}^{h} f(x)\phi_{2n+1}(x; -h, h; d\psi)d\psi \\ &= \int_0^{h^2} F_2(x)\phi_n(x; 0, h^2; d\psi_2)d\psi_2 \equiv f_{n,2}, \end{aligned} \tag{4}$$

where

$$F_1(x^2) = \frac{f(x) + f(-x)}{2}, \qquad xF_2(x^2) = \frac{f(x) - f(-x)}{2}. \tag{5}$$

We have further

$$f(x) = F_1(x^2) + xF_2(x^2) \sim \sum_{n=0}^{\infty} f_n\phi_n(x; -h, h; d\psi).$$

Making use of (3), (4) and (5), we get readily

$$\begin{aligned} F_1(x^2) &\sim \sum_{n=0}^{\infty} f_{2n}\phi_{2n}(x; -h, h; d\psi), \\ xF_2(x^2) &\sim \sum_{n=0}^{\infty} f_{2n+1}\phi_{2n+1}(x; -h, h; d\psi), \\ F_1(x) &\sim \sum_{n=0}^{\infty} f_{n,1}\phi_n(x; 0, h^2; d\psi_1), \\ F_2(x) &\sim \sum_{n=0}^{\infty} f_{n,2}\phi_n(x; 0, h^2; d\psi_2), \end{aligned} \tag{6}$$

$$\int_{-h}^{h} xF_1(x^2)F_2(x^2)d\psi = 0,$$

$$\int_{-h}^{h} f^2(x)d\psi - \sum_{n=0}^{\infty} f_n^2 = \left[\int_0^{h^2} F_1^2(x)d\psi_1 - \sum_{n=0}^{\infty} f_{n,1}^2\right] + \left[\int_0^{h^2} F_2^2(x)d\psi_2 - \sum_{n=0}^{\infty} f_{n,2}^2\right]. \tag{7}$$

By Bessel's inequality, *both brackets on the right side of* (7) *are non-negative*, and this directly proves the theorem stated.

REMARK. In the above discussion h may be assumed to be infinite, for closure always holds for a finite interval.

The most interesting application of the foregoing is to Hermite and Laguerre polynomials. In fact, it follows from the above theorem that the closure of both sequences

$$\{\phi_n(x; 0, \infty; e^{-x}x^{\alpha-1})\}, \quad \{\phi_n(x; 0, \infty; e^{-x}x^{\alpha})\}, \qquad \alpha \geqq 1/2,$$

implies that of $\{\phi_n(x; -\infty, \infty; e^{-x^2}|x|^{2\alpha-1})\}$, and conversely. In particular, taking $\alpha = 1/2$, we conclude that the closure of Hermite polynomials $\{\phi_n(x; -\infty, \infty; e^{-x^2})\}$ implies that either of the two sequences of Laguerre polynomials $\{\phi_n(x; 0, \infty; e^{-x}x^{-1/2})\}$, $\{\phi_n(x; 0, \infty; e^{-x}x^{1/2})\}$ is closed, and conversely.

THE UNIVERSITY OF PENNSYLVANIA